Department of Homeland Security Control Systems Security Program

(b)(6)
Deputy Director
Control Systems Security Program (CSSP)

Homeland Security

Agenda

- CSSP Introduction
- What are Industrial Control Systems?
- Threat Actors and Techniques
- Cyber Incident Examples
- Control Systems Security Program Overview
- Contact Information / Online Resources

Homeland Security

18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure into the following 18 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water and Water Treatment

Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system

Homeland Security

3

Control Systems Security Program

Mission Statement

To strengthen the control system security posture by coordinating across government, private sector, and international organizations in reducing the risk to Critical Infrastructure and Key Resources.

Homeland Security

4

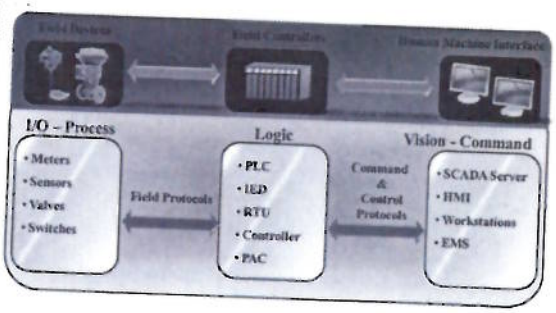
What are Industrial Control Systems?

The term "Industrial Control Systems" (ICS) refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- Any other automated / embedded system

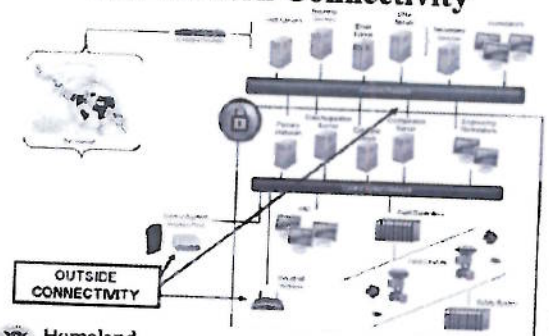
Homeland Security

ICS Communication Basics



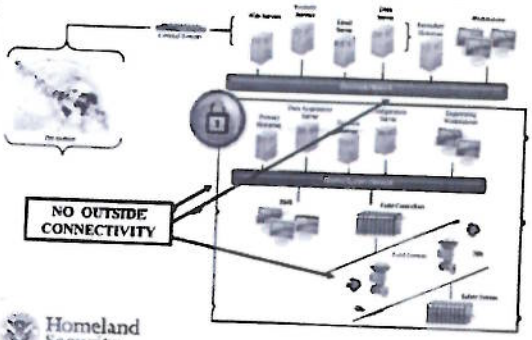
Homeland Security

ICS Modern Connectivity



Homeland Security

ICS Traditional Isolation



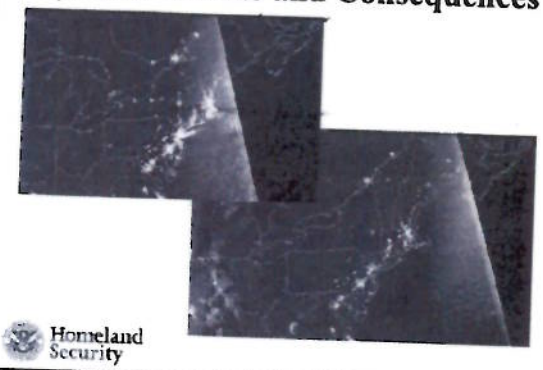
Homeland Security

Control Systems Security Challenges

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Antivirus & Mobile Code Countermeasures	Common & widely used	Can be difficult to deploy
Support Technology Lifetime	3 to 5 years	Up to 30+ years
Outsourcing	Common/widely used	Rarely used (vendor only)
Application of Patches	Regular/scheduled	Slow (vendor specific; compliance testing required)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are usually accepted	Critical due to safety
Availability	Delays are usually accepted	24 x 7 x 365 x forever (integrity also critical)
Security Awareness	Good in both private and public sector	Generally poor inside the control zone
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages / audit for event recreation
Physical Security	Secure	Traditionally good

Homeland Security

Cyber Incidents and Consequences



Homeland Security

USB Drives – Mariposa

Event:

- **An employee attended an industry event and used an instructor's USB to download presentation materials.**
- **The USB was unknowingly infected with the Mariposa botnet.**

Impact:

- **Over 100 computers at the employee's organization were infected**

Specifics:

- **When the employee returned to work and plugged the laptop into the network, the virus quickly spread**

Lessons learned:

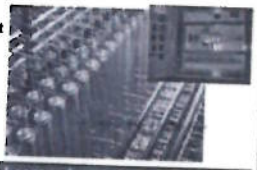
- Implement polices for analysis and use of USBs
- Isolate critical networks and implement controls for connections involving removable media

Homeland Security

Stuxnet

Event:

- **July 2010 - VirusBlockAda notifies Siemens of the discovered malware**
- **First malware known to specifically target a control system**



Impact:

- **Modifies PLC code and hides the changes from the operator**
- **Employed sophisticated evasion techniques**
- **Only impacted control systems operating variable frequency drives**

Specifics:

- **Highlighted the interdependencies and vulnerabilities that exist in legacy control system environments and demonstrated that motivated groups are interested in attacking CIKR sites**

Lessons learned:

- Be prepared to handle sophisticated malware by practicing defense-in-depth,
- Develop appropriate logging procedures, practice appropriate network monitoring, and be familiar with available resources for combating this type of event

Homeland Security

12

Spear-Phishing

- Multiple spear-phishing incidents in recent months involving major US Corporations
  - Banking
  - Oil & Gas
  - Water
- Emails are designed to look like intra –office traffic including company specific topics of concern
  - Actors use company websites and social media to do reconnaissance
  - Emails spoof actual account user names
- Main Goal: data exfiltration for industrial espionage and trade secrets

Lessons learned:
- Threat actors are becoming more sophisticated
- Common attack vector to gain a foothold
- Employ education and training

Homeland Security

13

DHS Mitigation Measures - CSSP

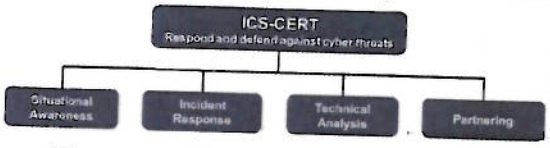
Homeland Security

Strategic Program Initiatives

- ICS-CERT - Industrial Control Systems – Cyber Emergency Response Team
- ICSJWG – Industrial Control Systems Joint Working Group
- Security Standards & Cybersecurity Evaluation Tool (CSET)
- Vendor Product Vulnerability Discovery
- Training & Workforce Development
- Site Assessment Visits
- Informational Products

Homeland Security

ICS Cyber Emergency Response Team



DIRECT Benefits to ICS and Critical Infrastructure

- Awareness of emerging issues and threats
- State of the art analysis capabilities specific to ICS
- Incident response support for recovery and future defense

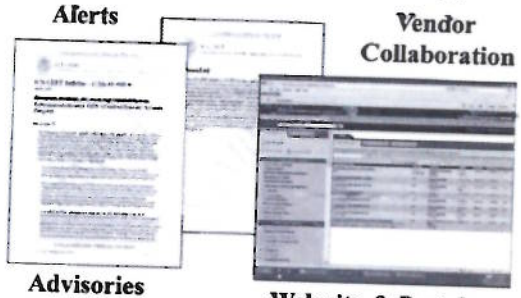
Homeland Security

ICS-CERT: A Unique DHS Capability

- Providing situational awareness
- Managing vulnerabilities in control systems technologies
- Performing incident response
- Conducting technical analysis
- Partnering with the control systems community

Homeland Security

ICS-CERT: Asset Owner Support



Homeland Security

18

Incident Response Support

- Onsite/offsite technical analysis and assistance
- Architecture analysis of network, control, and safety systems
- Exploit root cause and malicious activity analysis
- Mitigation strategy recommendations
- Coordination with Vendor Response Teams
- Threat information sharing

Homeland Security

Technical Analysis

- Vulnerabilities
- Malware
- Consequences
- Root cause
- Threat tactics and techniques
- Mitigation strategy effectiveness

Homeland Security

ICS – Joint Working Group

- Provides a vehicle for collaboration between government and private sector control systems stakeholders
  - Government Coordinating Council
  - Sector Coordinating Council
  - Subject Matter Experts
  - International Community

- Fosters information sharing and coordination of activities and programs across government and private industry stakeholders involved in protecting CIKR
- Includes 5 subgroups – 1 Pending
  - Vendors
  - International
  - Workforce Develop
  - Research and Development
  - ICS Roadmap Development
  - Pending (Standards and Metrics)

Homeland Security

Key Stakeholders

- **CI/KR Asset Owners**
- **Federal Sector Leaders**
- **Control Systems Vendors and Asset Owners & Operators**
- **Intelligence Community**
- **Law Enforcement**
- **State, Local, and Tribal Governments**
- **International Partners**

Homeland Security

Standards Improvement and Usage

Collaborations to evolve national and international standards for control system security

- Instrumentation, Systems, and Automation (ISA)
- National Institute of Standards and Technology (NIST)
- International Electrotechnical Commission (IEC)
- American Gas Association (AGA)
- American Pipeline Institute (API)

Homeland Security

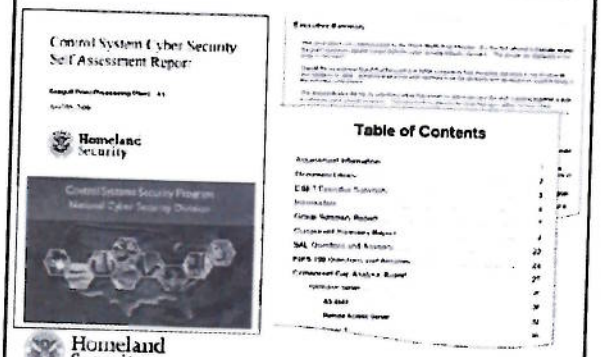
Cyber Security Evaluation Tool

- Software application
- Runs stand alone
- Assesses cyber security to known standards and recommendations

Include nuclear standard recently added (RG 5.71).

Homeland Security

Report – Status & Recommendations



Homeland Security

Vendor Product Vulnerability Discovery

- Working with major system vendors to identify vulnerabilities within components and software
- Vendors are developing remediation plans
- Currently developing a full-scale multi-vendor assessment configuration

Invensys EMERSON SIEMENS Honeywell OSI ABB

Homeland Security

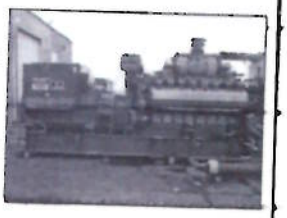
Control System Vendors

Rockwell Automation, Siemens, ABB, TPS, Vericom, OSI, GE, Cooper Power Systems, Stratus, Schneider Electric, wiredcity, EMERSON, LiveData, SISCO, AREVA, Honeywell, NOVATECH, SNC-LAVALIN, Online, SEL Schweitzer Engineering Laboratories, Inc.

Homeland Security

Aurora Vulnerability

- (2007) DHS assessment efforts discovered a potentially significant cross-sector vulnerability to Critical Infrastructure.
- Interagency team including Nuclear Sector Coordination Council (SCC) and NRC collaborated to assess knowledge gaps, further validate the risk, and publish plans to mitigate risk.



Homeland Security

Workforce Development

Web Based Training

- "Cyber Security for Control Systems Engineers and Operators"
- "Operational Security (OPSEC) for Control Systems"*

Instructor Led Courses

- Introduction to Control Systems Security for the Information Technology Professionals
- Intermediate Control Systems Security (Lecture and Workshop)
- Cyber Security Advanced Training and Workshop
- Control Systems Security for Senior Managers

International Training

- 30 countries have participated
- Provided basic, intermediate and advanced training

Homeland Security

Site Assessment Visits

- CSSP assists critical infrastructure asset owners in conducting self-assessments using the CSET.
- CSET provides a systematic and repeatable approach for assessing the security posture of industrial control & IT systems and networks including both high-level and detailed questions.
- CSSP encourages asset owners to identify their security gaps and implement the recommended mitigation strategies.
- All information protected as PCII.

Homeland Security

Site Assessment Observations

- **Weak or nonexistent cybersecurity policies and practices.**
  - Lack of a formal documented program and procedures
  - Need for an established cybersecurity team
  - Need for incident response and disaster recovery policies and/or directives
- **Insufficient control of remote logging and access.**
  - Weak enforcement of remote login policies
  - Weak port security
  - Network architecture not well understood and internal networks not segmented
  - Flat networks--devices not properly configured

Homeland Security

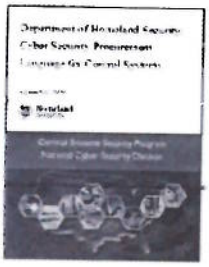
Risk Reduction Products

Cyber Security Procurement Language for Control Systems

Building Security into Control Systems

Provides sample or recommended language for control systems security requirements

- New SCADA/control systems
- Legacy systems
- Maintenance contracts
- Information and personnel security



Homeland Security

Contact Information

Report industrial control systems cyber incidents and vulnerabilities

- (b)(7)c, (b)(6)
-

Report general cyber incidents and vulnerabilities

- (b)(7)c, (b)(6)
-

Sign up for cyber alerts

- www.us-cert.gov

Learn more about Control Systems Security Program

-
-

Homeland Security

Chaney, Michael

From: (b)(6)
Sent: Friday, April 27, 2007 9:47 AM
To: (b)(6)

Subject: Latest revision
Attachments: Aurora Mitigation Strategy rev 3.doc

Importance: High

This is rev 3 of the mitigation document

We will step through this document today.

<<Aurora Mitigation Strategy rev 3.doc>>

(b)(5)

The Annex's at the back of this document are set up to contain just the Tiers' recommendations. These recommendations will be tracked by the Sector Coordinating Council for accountability purposes.

Remember
Engineers only call on Thursday at 10.

INEL
PNNL
E-SCC Engineers
N-SCC Engineers and Operators

PM overview call for all at 10Am on Friday

All are welcome

Authors call at 2PM on Friday.

Only volunteer authors (b)(6) or designee) and a few extras as you wish

Technical Assistant to the President CGG/Security
Deputy to the Chair - Nuclear Sector Coordinating Council
Deputy to the Vice Chair Partnership for Critical Infrastructure Security
(b)(6)

Control Systems Vulnerability—Aurora

(b)(6)

Director, Control Systems Security
National Cyber Security Division (NCSD)
U.S. Department of Homeland Security

Homeland Security

Agenda

Executive Summary

What is Aurora?

Significance and Impact of Aurora

CSSP Efforts to Address Aurora

Page 13 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Agenda

Executive Summary

What is Aurora?

Significance and Impact of Aurora

CSSP Efforts to Address Aurora

Homeland Security

What is Aurora?

Aurora is the malicious use of a protective relay or other digital protection and control device to inflict an out of sync condition that results in physical damage to rotational equipment

- The abrupt opening and closing of the protective circuit changes the behavior of the relay from providing maximum protection to inflicting maximum damage

INSERT SAWTOOTH GRAPHIC SEAN MENTIONED

Aurora is unique because the out-of-phase condition can be caused through a cyber attack

Homeland Security

Pages 16 through 17 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Agenda

Executive Summary

What is Aurora?

Significance and Impact of Aurora

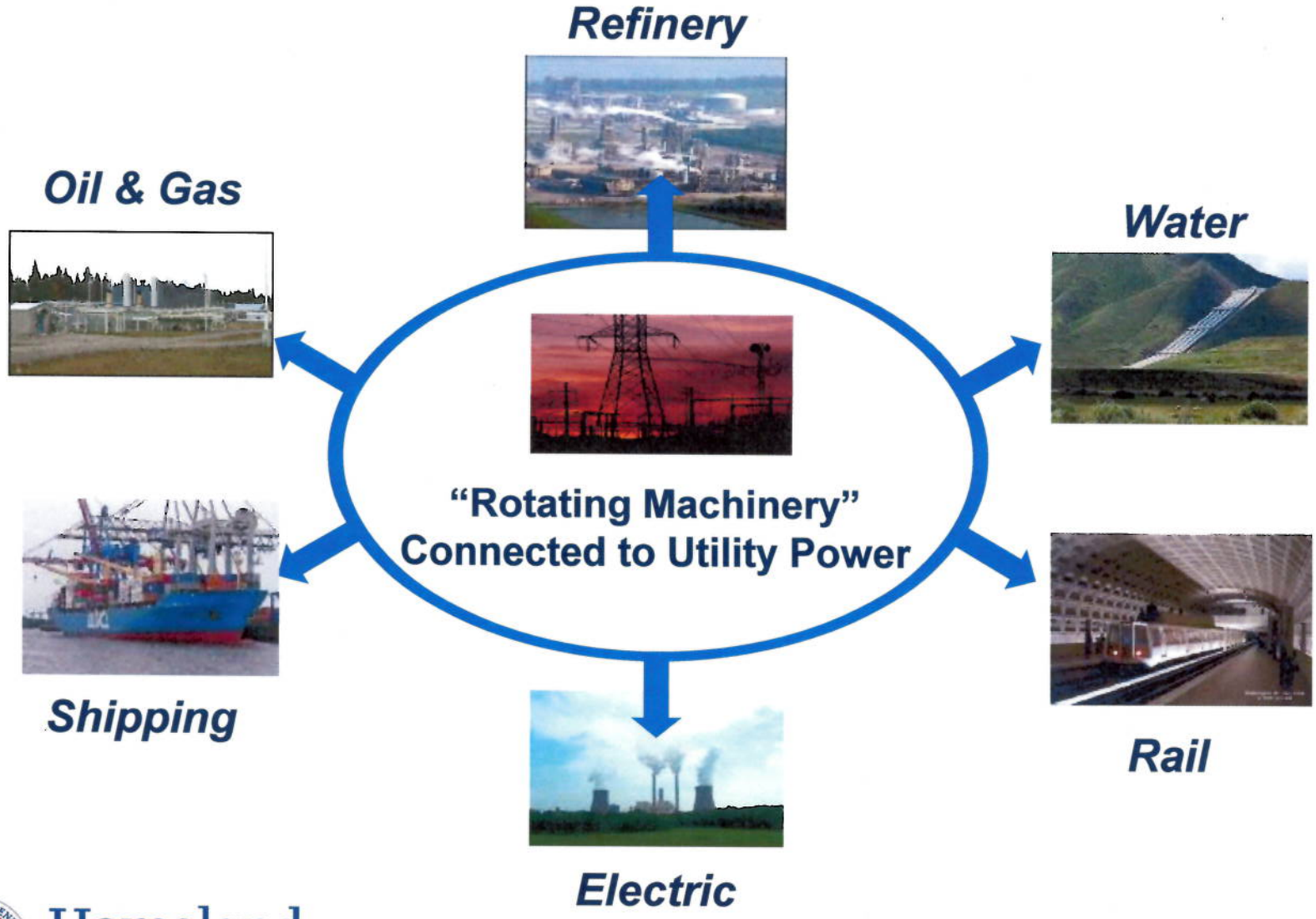
CSSP Efforts to Address Aurora

Homeland Security

Significance and Impact of Aurora

Homeland Security

Not Just An Electric Grid Problem



Homeland Security

Pages 21 through 22 redacted for the following reasons:
- -
(b)(5), (b)(7)f
(b)(7)f, (b)(5)

Agenda

Executive Summary

What is Aurora?

Significance and Impact of Aurora

CSSP Efforts to Address Aurora

Homeland Security

History of CSSP Involvement

<Graphical timeline showing the following elements>

- Discovery of Aurora vulnerability
- Field test to verify model predictions
- Disclosure of test results
- Mitigation development
- Work with sectors/stakeholders to implement mitigations

- Anything else I'm missing???

Field Test Objectives

Perform a test that demonstrates the potential vulnerability of equipment connected to the power grid, limited to single configuration

The test was conducted to confirm the vulnerability and impacts under real-world conditions

- The system under test was configured in a way that complies with industry best practices as confirmed by test participants prior to test execution

Data from the test was used to validate previous modeling and simulation results, demonstrate and catalog physical consequences, and provide a baseline for future tests

Test design was discussed with representatives of the Interagency Team, NERC, and TVA

Pages 26 through 28 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

AURORA Mitigation Timeline

2Q FY08 completed Aurora Event Checklist

- Checklist distributed to 6 sectors
  - The North American Electric Reliability Corporation (NERC) issued an Advisory for the Energy Sector.
  - Nuclear Regulatory Commission (NRC) issued an order for the Nuclear Sector.
  - Office of Infrastructure Protection distributed Checklist to Protective Security Advisors (PSAs).

3Q FY08

- Completed control systems security and Aurora training to PSAs

4Q FY08 PSA Assessment Technical Support

- Tennessee Valley Authority (TVA)
- Southwest Power Pool
- NASA's Kennedy Space Center
- City of Chicago Metropolitan Water Authority
- Northern New Jersey Water District

1Q FY09 PSA Assessment Technical Support

- Western Area Power Administration and Glen Canyon Site Assessment Visit
- Follow-up assessment at TVA facilities
- Multiple PSA assessments planned throughout FY09

Mitigation Efforts

Assisted sector-specific technical groups drafted Mitigation Plans with multi-tiered approach allowing for near, medium, and long term solutions

Reached out to protective relay vendors to propose mitigation steps such as improved access controls and modification of relay functionality

Engaged industry under the auspices of the Critical Infrastructure Partnership Advisory Committee (CIPAC)

Briefed Members of the House – and staff of the Senate – Homeland Security Committees as well as other interagency stakeholders.

International Coordination

- Industrial control systems representatives (United Kingdom and Canada) included in vulnerability validation efforts including validation test planning and preparations
- Shared information with Australia, Canada, New Zealand, and United Kingdom to provide insight into risk assessment and mitigation planning
- Allies notified of impending press release of vulnerability

CIKR Sectors of Concern

Sector	SCC Briefed	Mitigation Development Date	Mitigation Distribution Date
(b)(7)f, (b)(5)	June 2007	September 2007	September 2007
	June 2007	September 2007	September 2007
	June 2007	October 2007	October 2007
	February 2007	June 2007	June 2007
	February 2007	May 2007	June 2007
	June 2007	September 2007	September 2007
	June 2007	September 2007	September 2007

2007 & 2008

- IP/POD/PSCD/NCSD Aurora briefings and technical assistance to SCCs, SSAs, CIKR facilities
- PSCD – ECIP assist visits to Tier I & Tier II facilities
- PCIS – 50 + briefings and technical assistance to CIKR sectors and facilities

Homeland Security

Pages 33 through 39 redacted for the following reasons:
- -
(b)(7)e, (b)(5)
(b)(7)f, (b)(5)

AURORA Sector Milestones

(b)(7)f, (b)(5)

(b)(7)f, (b)(5)

Mitigation measures tracked and evaluated by Sector Specific Agencies (SSA).

Homeland Security

AURORA Nuclear Sector Milestones

(b)(7)f, (b)(5)

Mitigation Measures validated by NRC through direct reporting and site visits. 100% complete

Homeland Security

Page 42 redacted for the following reason:
- -
(b)(5), (b)(7)f

AURORA Metrics Process

A comprehensive data base was developed to track mitigation inspection results across all sectors.

Comprehensive checklist distributed to PSAs and asset owner/operators.

Control Systems Cyber Security Self-Assessment Tool (CS^2SAT) evaluations conducted during on-site visits in coordination with Site Assessment Visits (SAV) and Comprehensive Review (CR) process.

Incorporate AURORA checklist within the CS^2SAT for data capture purposes.

Page 44 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Aurora Vulnerability

Mitigation Strategy

Introduction

AURORA (the "Vulnerability") is a recently discovered vulnerability affecting spinning machines (motors, generators, compressors, etc.) that are directly coupled to the electric power grid. This discovery requires a rapid and organized response to develop mitigation to reduce and eventually eliminate this risk. The Vulnerability pertains to devices called digital protective relays, programmable logic controllers, and bay controllers. These devices are common protection and control devices found in electric grid substations. These devices are designed to autonomously manage fluctuations or anomalies in the power grid and protect critical infrastructure from damage. In a normal, intended use scenario, protective relays disconnect faulty sections of the power system from the remaining healthy portions in order to protect electrical power generation devices. However, what the vulnerability testing has demonstrated is that certain digital protective relays are capable of being changed from protective to a destructive devices.

Purpose

The purpose of this Private Sector strategy is to develop and implement an Aurora Vulnerability mitigation strategy that is deliberative and collaborative. The specific intent of this strategy is to;

- Increase the requirements (skills, tools and knowledge) needed to exploit the technology platforms we are concerned with:
  - Strengthen access controls to Aurora critical devices
  - Set alarms for all remote access to relays
  - Separate the functionality of configuration and read/control
- Vary the environment to limit the scalability of an attack (Diverse defense in depth)
  - Develop a hardwire breaker timing sequence to prevent re-close for some breakers
  - Other technical options depending on power system topology to further reduce the scalability or to protect specific point targets.
- Provide high-assurance technical mitigation for high consequence facilities.
  - Deploy devices that can detect a possible Aurora attack and isolate the rotating machinery.
  - Other technologies that can provide device specific protection.

To achieve this purpose, these mitigation efforts will be divided into four tiers that adhere to security in depth. This division allows initiation of Short-Term actions to reduce the Vulnerability while Long-Term actions are being developed, tested and implemented.

- Tier I: Very short term recommended practices - Goal: 2QFY07 - Coordinate with asset owners and regulators to enhance industry practices to reduce the scope of potential access to digital devices and to improve monitoring and response capabilities.
- Tier II: Mid-term - 2 to 6 months. Hardware mitigation - Goal: 3QFY07 – Develop and deploy hardware protective devices capable of mitigating the vulnerability.
- Tier III: Long-term – 6 to 18 months. Software mitigation - Goal: 4QFY07 - Coordinate with vendors to develop software modifications in existing and future digital protective relays that will further support the Tier II vulnerability mitigation.
- Tier IV: Very long-term and future steady state. PCIS and GCCs' develop recovery strategies from regional effects of very prolonged disruptions.

This approach will provide some capability to manage the risk over the mid to long term.

Scope

Develop short, mid, and long term recommended mitigations to reduce the risk associated with unauthorized remote access to protection and control devices that can result in physical damage to infrastructure.

Other areas of concern may become apparent during this effort but they will only be captured

Approach

The vulnerability demonstrated in the DHS directed Aurora Generator Test requires a multi-pronged effort with some elements' aimed at mitigating the exposure to the vulnerability or limiting the range of an exploit of it and an element designed to prepare long-term efforts for recovery from either a successful exploit or accidental Aurora exploit. The vulnerability mitigation efforts can be thought of in the following areas;

- Increase the requirements (skills, tools and knowledge) needed to exploit the technology platforms we are concerned with,
  - Strengthen access controls to Aurora critical relays
  - Set alarms for remote access to relays
  - Separate the functionality of configuration and read/control
- Vary the environment to limit the scalability of an attack (Diverse defense in depth)
  - Implement a timing sequence to prevent re-close for some breakers hardwire breaker timing sequence to prevent re-close for some breakers. These devices would be simple and not connected to external communications.
  - Other technical options depending on system topology to further reduce the scalability or to protect specific point targets.
- Provide high-assurance technical mitigation for high consequence facilities.
  - Deploy devices that can detect a possible Aurora attack and isolate the rotating machinery.
  - Other technologies that can provide device specific protection.

These mitigation efforts are aimed at "raising the bar" so that it takes much more effort to access substation equipment remotely (security solutions, procedure changes, limit access, etc.), varying the exploitability of the vulnerability to reduce the potential scalability of an attack (large utility systems having one vulnerable path to exploit multiple substation devices).. At the heart of these efforts is a device, installed within the customer's fence, that can sense an attack and open supply-side breakers to isolate the rotating equipment prior to it being damaged (a design is in the works called the Rotating Equipment Isolation Device).

The execution of this mitigation strategy will use a four tiered approach with three of these tiers focused on Short, Mid, and Long-term mitigation strategies. The fourth tier is focused on recovery activities should this vulnerability be intentionally or accidentally exploited.

The elements of the three areas of focus, Increase Effort Needed, Vary Environment to Limit Scalability, and Point solutions for Critical Devices, are parsed into one or more of the following tiers based on complexity issues involved.

This multi-Tier approach also takes into consideration the balance between losing control of the information and reaching a wide enough audience at the right time. (Many of the device suppliers are foreign owned entities or have significant foreign soil influenced product development).

The following sections describe the four mitigation effort tiers of mitigation efforts.

Tier I – Short Term Mitigation Measures: Goal 45 to 60 days

Due to the short time frame, Tier I efforts are restricted to enhancing existing utility/industrial system practices, standards and regulations (possibly via either Relief's granted or Orders made) within critical infrastructure sectors as they pertain to remote access to Aurora critical relay devices. The Private sector, operating under the Sector Partnership Model, will coordinate with the Department of Homeland Security's Control Systems Security Program (CSSP) and the Infrastructure Partnership Division (IPD). The CSSP and IPD will ensure that the Private Sectors' efforts with asset owners are coordinated with the various involved Government Coordinating Councils (GCCs).

The N-SCC and E-SCC will develop enhancements or recommended mitigation practices focused on measures to restrict unauthorized access to digital devices within substations, to improve monitoring of attempted access to these digital devices, and to build capabilities to respond to intrusion attempts.

Within DHS, CSSP will support IPD in coordinating with GCCs for both the Electric and Nuclear Sectors to ensure that there are no governmental impediments for swift implementation to these critical Short-Term strategies

The Tier I recommendations are focused on reducing the scope of potential access to digital protective relays and to improve monitoring and response capabilities. The details of these recommendations are contained later in this report.

The N-SCC, E-SCC and their GCC counterparts will ensure the following:

- The N-SCC and E-SCC will develop enhancements or recommended mitigation practices focused on measures to restrict unauthorized access to digital protective relays, to improve monitoring of attempted access to digital protective relays, and to build capabilities to respond to intrusion attempts. **[Timeline – 45 business days]**
- The N-SCC and E-SCC will use the PCIS to coordinate the outreach to other SCCs. **[Timeline – 45 business days**
- CSSP will support IPD in coordinating with sector GCCs and the Federal Control Systems Security Working Group for further vetting and validation of recommended mitigation measures **[Timeline – 60 days].**
- CSSP will support IPD coordination with regulatory entities for consideration of recommended enhancements to standards and regulations. The goal will be for regulatory entities to approve enhanced mitigation measures in current regulatory infrastructure. **[Timeline – 90 days**].
- CSSP will support US-CERT in outreach to U5 Countries (U.S., Canada, United Kingdom, Australia, and New Zealand) to share planned enhancements to industry recommended practices. **[Timeline – 90 days].**

Tier II – Mid-Term Mitigation – Goal 60 day to 180 days

The goal of Tier II is to develop and implement more complicated mitigation measure in the areas of Increase Effort Needed, Vary Environment to Limit Scalability, and Point solutions for Critical Devices. These efforts will require more resources and planning in order to accomplish the goals in these areas.

THE DHS research has provided insight into the trigger associated with launching a cyber attack on protective relays. Initial studies determined that there are some protective relays that provide users with

sufficient programmability to alter the device such that the synchronism detection is changed from being a healthy "in-synchronism" condition (normal operations) to one where an "out-of-synchronism" (abnormal operations) is improperly declared as normal.

Tier II focuses on developing both hardware modifications or new devices and software modifications that are capable of mitigating this vulnerability.

There are also other examples such as toughening the Access Controls and making changes through the Vendor community that accomplish one or more of the three objectives.

(b)(7)f, (b)(5)

(b)(7)f, (b)(5)

Tier IV – Long-Term Recovery Strategies

Insert FEMA like language here

Tier I – Short Term Mitigation Measures: Goal 45 to 60 days

Recommendations

Very short term recommended practices - Goal: 2QFY07 - Coordinate with asset owners and regulators to enhance industry practices to reduce the scope of potential access to digital protective relays and to improve monitoring and response capabilities.

Remove all Communications to relays

Description: Add words

Focus: Add Word

Requirements: Add Words

Benefits: Add words

Barriers/Constraints: Add words

Opportunities for Accelerating: Add Words

Protection Rating/Risk Reduction: Add Rating

Remove Remote Access but leave SCADA

Description: Add words

Focus: Add Word

Requirements: Add Words

Benefits: Add words

Barriers/Constraints: Add words

Opportunities for Accelerating: Add Words

Protection Rating/Risk Reduction: Add Rating

Alarm for access to relay

Description: Add words

Focus: Add Word

Requirements: Add Words

Benefits: Add words

Barriers/Constraints: Add words

Opportunities for Accelerating: Add Words

Protection Rating/Risk Reduction: Add Rating

Disconnect Communications to all Aurora critical Devices

Description: Add words

Focus: Add Word

Requirements: Add Words

Benefits: Add words

Barriers/Constraints: Add words

Opportunities for Accelerating: Add Words

Protection Rating/Risk Reduction: Add Rating

Separate the functionality

Description: Add words

Focus: Add Word

Requirements: Add Words

Benefits: Add words

Barriers/Constraints: Add words

Opportunities for Accelerating: Add Words

Protection Rating/Risk Reduction: Add Rating

Isolate EDG from grid

Description: Approach key end-users (Nuclear sector, water, etc.) and request that they take the following steps: 1. do not parallel backup generators (if possible) to the grid when in use; and 2. randomize generator testing.

Focus: End users

Requirements: Modify operating procedures

Benefits: Keeps backup generators from being exposed to the energy source capable of damaging them if they are not connected to the power grid.

Barriers/Constraints: Diesel generator loading requirements are complicated: i.e. full load operation may not be available without the addition of sizeable loading banks. This mitigation only protects customer-owned generation. Diesel generators need to be periodically run at full load to ensure they will reliability operate when needed in an emergency. Often the only way to accomplish this is to parallel them to the grid in order to run them under full load. Installing load banks to circumvent this requirement is a long-term solution that is very expensive.

Opportunities for Accelerating:

Protection Rating/Risk Reduction:

(b)(7)f, (b)(5)

Pages 53 through 56 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Focus:

Requirements:

Benefits:

Barriers/Constraints:

Opportunities for Accelerating:

Protection Rating/Risk Reduction:

Firmware changes

Description: Enforce the zero degree relative phase angle when breaker is closed.

Focus: Vendor

Requirements:

Benefits:

Barriers/Constraints:

Opportunities for Accelerating:

Protection Rating/Risk Reduction:

Strong password and protocols

Description:

Focus:

Requirements:

Benefits:

Barriers/Constraints:

Opportunities for Accelerating:

Protection Rating/Risk Reduction:

Strong Access Controls

Description:

Focus:

Requirements:

Benefits:

Barriers/Constraints:

Opportunities for Accelerating:

Protection Rating/Risk Reduction:

Implement strong passwords across the system

A strong password contains special characters, upper and lower case, is eight or more characters in length, is not a dictionary word, etc. Password policies should be adopted across energy sector.

Pages 58 through 62 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Tier IV Recommendations

Page 1 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)f, (b)(5)

Pages 3 through 24 redacted for the following reasons:
- -
(b)(5), (b)(7)f
(b)(7)f, (b)(5)

Battelle Energy Alliance (BEA)

COST ESTIMATE SUPPORT DATA RECAPITULATION

Project Title:	Aurora Generator Test
Estimator:	R. R. Honsinger
Date:	February 13, 2007
Estimate Type:	Class 3
File:	9A17
Approved By:	

I. **PURPOSE:** *Brief description of the intent of how the estimate is to be used, i.e., for engineering study, comparative analysis, DWP, LCB out-year planning, BCP, etc.*

The estimate is prepared to support full project funding requests.

II. **SCOPE OF WORK:** *Brief statement of the project's objective. Thorough overview and description of the proposed project. Identify work to be accomplished, as well as any specific work to be excluded.*

The objectives of this project are to perform research and development (R&D) operational tests of a diesel generator system.

These objectives will be accomplished by:

1. Procurement of a 13.8 KV 2.25 MW diesel powered generator.
2. Perform site assessment for location of test pad area.
3. Engineering design of 95' by 75' test pad area.
4. Construction of test pad area including concrete equipment pads.
5. Electrical engineering design for connection of diesel generator to existing substation.
6. Construction to connect diesel generator to existing substation equipment.
7. Conduct environmental impact review.
8. Conduct safety analysis and develop safety documentation.
9. Perform modeling/simulation of electrical tests.
10. Develop test procedures.
11. Develop quality, safety, security, and emergency plans.
12. Conduct system test and document test results.
13. Conduct post test maintenance.
14. Perform equipment removal and site cleanup.
15. Provide project management, construction management, and project control.

Specific work scope excluded:
none

III. **BASIS OF THE ESTIMATE:** *Overall methodology and rationale of how the estimate was developed. Source documents to include drawings, design reports, engineers' notes and/or other documentation upon which the estimate is originated. Overall explanation of sources for resource pricing.*

A. Project scope was based upon project team meetings, a preliminary project schedule and work breakdown structure, and preliminary engineering drawings for the test pad construction.
B. Construction costs were estimated using a semi-detailed unit cost method.
C. The diesel generator costs were based upon a supplier quote.
D. Engineering costs are based upon input from the BEA Engineering Services Division and the BEA Power Management organization.
E. Test procedure development costs were based upon engineering judgments provided by the BEA lead personnel assigned to develop the test procedures.
F. Modeling/simulation costs were based upon engineering judgments provided by the personnel assigned to perform the modeling/simulation.
G. Safety analysis and environmental documentation costs were based upon engineering judgment of personnel assigned to perform the activities and estimator judgment.
H. Costs to perform the system tests are based upon the engineering judgment of the project team and the estimator.
I. Costs to perform post testing and maintenance activities are based upon engineering judgment of the project electrical engineers and were based upon previous experience with high voltage switch gear replacement and INL substation maintenance.
J. Costs to perform the equipment removal and site cleanup are based upon estimator judgment and input environmental support personnel.
K. A review of the estimate was performed by members project team responsible for the major estimate activities.

IV. **ASSUMPTIONS:** *Condition statements accepted or supposed true without proof of demonstration; statements adding clarification to scope. An assumption has a direct impact on total estimated cost.*

A. It is assumed that BEA personnel will perform all of the design, documentation, and supervision. It is also assumed that BEA personnel will be available to complete this work.
B. An informal design review will be performed.
C. Provisions have been made for subcontracted work. It is assumed that the construction work will be performed by local subcontractors experienced with similar work at the INL Site. Subcontractor personnel are assumed to be fully trained to perform the construction activities of this project. All subcontractors will be pre-approved.

D. Hazardous materials and radiological contamination will not be encountered during this project.
E. No obstacles will be encountered during excavation for test pad construction.
F. This project is assumed to be Block 4 in the Nine Block Matrix (Safety Risk/Operational Interface). A full time non-working superintendent is required.
G. The construction of the test pad will be complete within one week period.
H. Concrete will be a high strength fast cure mix.
I. All required building materials will be available in the time frame of the project schedule.
J. Equipment procurement schedules and delivery will support the test date.
K. Modeling and simulation activities will show no adverse impacts to the INL power system infrastructure.
L. Project will proceed as scheduled at the time of estimate preparation and the test will occur as scheduled.

V. **CONTINGENCY GUIDELINE IMPLEMENTATION:** *Explanation of methodology used in determining overall contingency. Identify any specific drivers or items of concern.*

Contingency has been applied to this estimate. The estimate is based upon a conceptual level evaluation and determination of the proposed project scope. This level of project development inherently includes risks which should be mitigated by the addition of contingency dollars. The contingency rates were developed by the estimator and the project team. A formal risk analysis was not performed.

Risk and contingency were evaluated and applied at a high level within the estimate. The project summary report shows the percentage of contingency assigned to the various activities of the estimate. Low risk activities such as generator procurement were assigned a 5% contingency. The higher risk activities were assigned contingency rates ranging from 30% to 75%

Total Project Contingency has been calculated to be 32%.

Items of risk considered for these calculations include but are not limited to:

A. Construction costs are subject to impacts due to adverse weather, material delivery delays, engineering design changes, and incomplete scope definition at time of estimate preparation.

B. Project management, construction management, and support services can be impacted by delays in the project schedule. A few days delay in a short duration execution period can result in a substantial increase in cost.

C. Equipment procurement is a high risk activity because some component selections and specifications were not available at the time of estimate preparation.
D. Modeling and simulation development and validation is recognized as high risk due to the variability and unknowns associated with the validations process and requirements.
E. Test procedure development is high risk due to the complexity of the test requirements, and the high level of interface required between all of the affected organizations.
F. Post testing and maintenance is a high risk activity due to the unknown affects that may result from the generator tests and limited scope definition. Replacement of damaged switch gear at substation #2 is included in the estimated cost.

Items of risk not considered for inclusion in the project contingency include:

A. Catastrophic failure or damage to Substation #2 transformers has not been included in the estimated costs. The cost to replace a substation transformer has been estimated by the INL power systems engineers to cost as much as $1,000,000. The likelihood of a failure of this type has been evaluated by INL engineers and is viewed as a low probability.
B. Damage to electrical infrastructure components at other INL facilities due to impacts from this test. The likelihood of a failure of this type has been evaluated by INL engineers and is viewed as a low probability.

VI. **ESTIMATE SUMMARY**: *Total dollars/hours and Rough Order Magnitude (ROM) allocations of the methodologies used to develop the cost estimate.*

Estimate Methodology	ROM Percentage %
Project Team	70
Recorded Actuals	0
Parametric	0
Vendor Quotes	20
Other (RS Means)	10
TOTAL	100

VII. **OTHER COMMENTS/CONCERNS SPECIFIC TO THE ESTIMATE:**

None

Project Name: ***Aurora Generator Test***

Project Location: ***INL***
Estimate Number: ***9A17***

Project Summary Report

Client: ***L. E. Goldman, 6-0010***
Prepared By: ***R. R. Honsinger***
Estimate Type: ***Class 3***

Level	Description	Estimate Subtotal	Escalation	Contingency	Contingency %	TOTAL
	Project Management (PM)	$355,620	$0	$106,686	30.00%	$462,306
	.... BEA Project Management	$195,620	$0	$58,686	30.00%	$254,306
	.... Industrial Experts and Consultants	$160,000	$0	$48,000	30.00%	$208,000
	Generator Procurement	$371,000	$0	$18,550	5.00%	$389,550
	Site Assessment and Walk-down	$6,000	$0	$300	5.00%	$6,300
	System Engineering and Design	$86,942	$0	$26,083	30.00%	$113,024
	.... System Engineering and Design	$86,942	$0	$26,083	30.00%	$113,024
	Equipment Procurement	$85,560	$0	$64,170	75.00%	$149,730
	Construction and Installation	$309,086	$0	$87,869	28.43%	$396,956
	.... Construction - Pad and Barrier Construction	$156,224	$0	$31,245	20.00%	$187,468
	..... General Conditions	$14,065	$0	$2,813	20.00%	$16,878
	..... Sitework	$34,542	$0	$6,908	20.00%	$41,450
	..... Concrete	$72,228	$0	$14,446	20.00%	$86,674
	..... Masonry	$35,389	$0	$7,078	20.00%	$42,466
	.... Equipment Installation	$107,659	$0	$43,064	40.00%	$150,722
	..... Mechanical - Subcontractor	$6,040	$0	$2,416	40.00%	$8,456
	..... Install Generator Fuel and Cooling Systems	$6,040	$0	$2,416	40.00%	$8,456
	..... Electrical - Subcontractor	$57,325	$0	$22,930	40.00%	$80,254
	..... Install Diesel Generator	$15,885	$0	$6,354	40.00%	$22,238
	..... Install Cable	$21,980	$0	$8,792	40.00%	$30,771
	..... Remove Generator and Cable	$19,460	$0	$7,784	40.00%	$27,245
	..... Electrical - BEA	$44,294	$0	$17,718	40.00%	$62,012
	..... Hookups at Substation	$19,599	$0	$7,840	40.00%	$27,439
	..... Install Test Equipment	$9,415	$0	$3,766	40.00%	$13,181
	..... Install Video/TV Capture Equipment	$9,415	$0	$3,766	40.00%	$13,181

Project Summary Report

Project Name: ***Aurora Generator Test***

Project Location: ***INL***
Estimate Number: ***9A17***

Client: ***L. E. Goldman, 6-0010***
Prepared By: ***R. R. Honsinger***
Estimate Type: ***Class 3***

Level	Description	Estimate Subtotal	Escalation	Contingency	Contingency %	TOTAL
	..... Disconnect from Substation	$5,865	$0	$2,346	40.00%	$8,210
	.... Construction Management (CM) and Support	$45,204	$0	$13,561	30.00%	$58,765
	Equipment Pre-Test	$16,000	$0	$6,400	40.00%	$22,400
	.... Generator Pre-Test	$16,000	$0	$6,400	40.00%	$22,400
	Modeling/Simulation	$47,400	$0	$18,960	40.00%	$66,360
	.... Model/Simulation Program Development	$47,400	$0	$18,960	40.00%	$66,360
	Safety Analysis	$39,000	$0	$7,800	20.00%	$46,800
	.... Develop Safety Documentation	$27,000	$0	$5,400	20.00%	$32,400
	.... Conduct Safety Analysis	$12,000	$0	$2,400	20.00%	$14,400
	Environmental Documentation	$33,000	$0	$6,600	20.00%	$39,600
	.... Conduct Environmental Impact Review & Environmental Support	$33,000	$0	$6,600	20.00%	$39,600
	Procedure Development	$141,300	$0	$56,520	40.00%	$197,820
	.... Equipment Test Procedures Development	$43,800	$0	$17,520	40.00%	$61,320
	.... Instrumentation Test Procedures Development	$27,000	$0	$10,800	40.00%	$37,800
	.... Emergency Plan Development	$18,000	$0	$7,200	40.00%	$25,200
	.... Equipment Removal/Site Cleanup Plan	$18,000	$0	$7,200	40.00%	$25,200
	.... QA Plan	$10,500	$0	$4,200	40.00%	$14,700
	.... OPSEC Plan	$18,000	$0	$7,200	40.00%	$25,200
	.... Security/Classification Plan	$6,000	$0	$2,400	40.00%	$8,400
	System Test	$110,260	$0	$44,104	40.00%	$154,364
	.... Conduct Equipment Test	$70,660	$0	$28,264	40.00%	$98,924
	.... Documentation of Test Results	$39,600	$0	$15,840	40.00%	$55,440
	Post Testing /Maintenance	$377,060	$0	$188,530	50.00%	$565,590
	.... Conduct Post Testing and Maintenance	$377,060	$0	$188,530	50.00%	$565,590

Project Summary Report

Project Name: ***Aurora Generator Test***

Project Location: ***INL***
Estimate Number: ***9A17***

Client: ***L. E. Goldman, 6-0010***
Prepared By: ***R. R. Honsinger***
Estimate Type: ***Class 3***

Level	Description	Estimate Subtotal	Escalation	Contingency	Contingency %	TOTAL
	Site Cleanup and Equipment Removal	$79,060	$0	$31,624	40.00%	$110,685
	.... Equipment Removal Site Restoration	$79,060	$0	$31,624	40.00%	$110,685
	..... Remove Generator and Cable	$29,460	$0	$11,784	40.00%	$41,245
	..... Remove Blocks and Conc Pad	$30,000	$0	$12,000	40.00%	$42,000
	..... Environmental and WGS Support	$19,600	$0	$7,840	40.00%	$27,440
	BEA Material Handling Fee and G&A	$66,750	$0	$6,675	10.00%	$73,425
	Work For Others (WFO) Fees	$63,000	$0	$18,900	30.00%	$81,900
Total	Aurora Generator Test	$2,187,038	$0	$689,771	31.54%	$2,876,809

Aurora

Generator Test

Video Summary

~~OFFICIAL USE ONLY~~
Contains information which may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number 2
Approval by the Department of Energy is required prior to public release.

Reviewed by Robert Polk, 03/06/2007

6 March 2007

The video footage is that of a large, 27 ton diesel generator (4,000 lbs heavier than a M3 Bradley Infantry Fighting Vehicle) being subjected to tremendous over-torque stresses that eventually led to its destruction.

> The over-torque stress was induced by creating an out-of-sync condition between the generator and the power grid. The out-of-sync condition was created via a cyber attack against a substation device that is meant to prevent this condition from occurring. A close, but imperfect, analogy would be to imagine the effect of shifting a car into Reverse while it is being driven on a highway, or the effect of revving the engine up while the car is in neutral and then shifting it into Drive.

The test was already in progress as the video starts and the generator had already been subjected to several "hits" from the attack.

Each time the out-of-sync condition is created, the over-torque causes this 27 ton machine to bounce or jolt. The machine has protections from torque built in, like the spring mounts, a flexible coupling or grommet designed to absorb vibration, etc (different machines do not have these protections and would show the effects of this torque earlier). As each jolt occurs, you can see material begin to fall off or get ejected.

The black pieces being ejected are that of a heavy rubber-based coupler or grommet as it is being ripped apart from the stress. The coupler connects the 16 cylinder diesel motor to the generator. It is a factory installed part intended to reduce vibration and absorb stress between that connection.

The effects of the stress are cumulative and begin to take their toll on the machine.

The coupler disintegrates further with each iteration. More pieces are ejected.

The diesel engine begins to experience damage.

The video culminates with the destruction of the diesel and the coupler.

Initial post-test observations indicate damage to the generator as well.

The unit was destroyed in approximately three minutes.

There were intentional pauses between each iteration of the attack in order to assess damage and maintain safety protocols. An actual attack could have been conducted much faster.

Control Systems Security

Aurora Update Brief

Agenda

- Executive Summary
- Aurora Project Review
- Knowledge Gaps
- Current Status
- Next Steps

Aurora Project Review

- A vulnerability was discovered and an Interagency Tiger Team was formed
- Initial concerns and modeling results were confirmed by a physical test March 4 2007
- Test resulted in a total loss of generating capability with extensive damage in about 3 minutes
- A strong example of interagency cooperation and public-private partnership

Homeland Security

Knowledge Gap Assessment

- Tiger Team will work with industry partners to identify current unknown critical information needed to assess the risk and develop a work plan for risk mitigation:
    - Identify protective relays and other devices that may be susceptible to this exploitation
    - Identify currently installed base of vulnerable relays
    - Identify exposure of this installed equipment to physical and remote access
    - Identify security technologies and procedures currently in place
    - Identify and evaluate applicable standards
    - Determine effectiveness of security technologies and procedures presently installed
    - Determine sensitivity of the scenario parameters
    - Determine susceptibility of rotating equipment damage as a function of distance from the event initiation
    - Conduct an inspection of a statistically relevant number of “protective relays” to determine any type of existing physical or cyber exploitation or compromise

Mitigation – Next Steps

- Greatest potential for exploitation of the vulnerability exists in the electrical sector; concentrating efforts there first
- Tiger Team will work jointly with Industry through the Sector Coordinating Councils (SCC) addressing the following:
  - Identify resources from Private Sector needed to address the knowledge gaps listed on the previous slide.
  - SCCs will establish task groups to work with the Aurora Tiger Team to address the list of knowledge gaps.
  - Clarify the extent of risk associated with the Aurora vulnerability.
  - Develop appropriate, cost-effective mitigation solutions.
  - Leverage multiple venues to disseminate mitigation solutions to ensure engagement of all components of a sector (e.g., trade associations).
- Tiger Team will work with the Electric and Nuclear sectors first, and then reach to other sectors as determined.
- Tiger Team will then reach out to appropriate protective relay vendors to enhance vendor understanding of possible risks associated with the Aurora Vulnerability, to encourage modifications to protective relay functionality, and to facilitate notification to affected industry sectors.

Homeland Security

Pages 7 through 9 redacted for the following reasons:
- -
(b)(5)

AURORA:
The Power Grid as an Attack Vector

May 7, 2007

Homeland Security

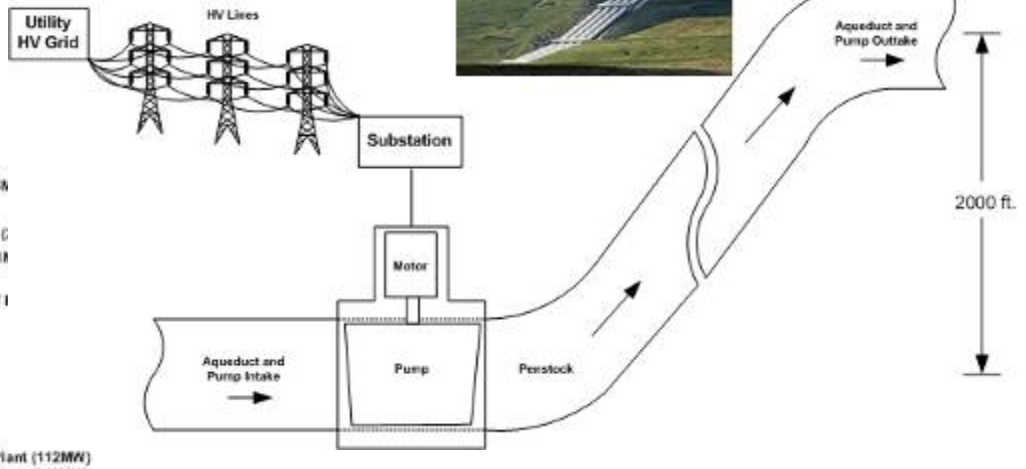
Agenda

- Vulnerability Overview
- Tiger Team Tasks
- Tiger Team Level of Concern/Impact
- Threat Assessment
- Risk Assessment
- Next Steps
- Industry Interaction
- Mitigation Plan

Pages 12 through 16 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

AURORA Vulnerability Example

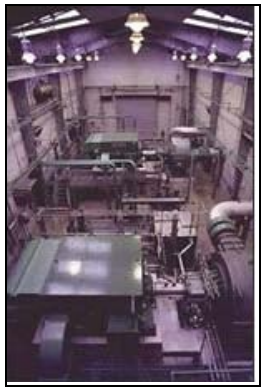
Water Pumping Plants Use Large Motors in Series

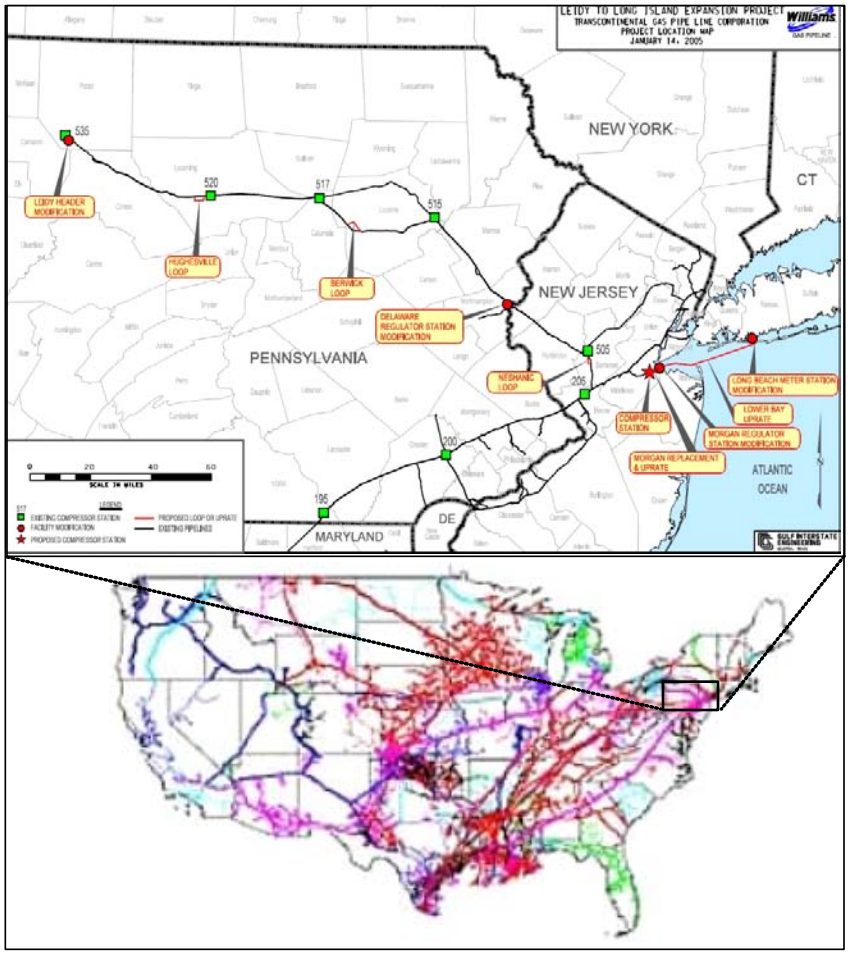


Homeland Security

AURORA Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities





Homeland Security

Other Vulnerable Infrastructure

- Government Facilities / Bases
- AC Train Grids
  - Cyclo-converters
- Continuous Pour Steel Mills
  - Power interruption
- Refineries
- Chemical Plants
  - Process control equipment
- Municipalities
  - Large induction motor pumps
- Financial Markets / Telecommunications
  - Air conditioning units

Homeland Security

AURORA Threat Assessment

Provided by HITRAC - ~~SECRET~~ Briefing

Homeland Security

AURORA Risk Assessment

Provided by IP/RMD - ~~SECRET~~ Briefing

Homeland Security

Tiger Team

- U/S Foresman directed the formation of a Tiger Team to scope the vulnerability, threat, and risk of the AURORA scenario
- Tiger Team response indicated a reason for concern and U/S Foresman established a milestone for a physical test
- Tiger Team was expanded from Federal stakeholders to include representatives from private industry
  - North American Electrical Reliability Corporation
  - Tennessee Valley Authority
  - Electric Sector Coordinating Counsel
- Execute the test and evaluate results quickly then develop mitigation strategy based on the result

Homeland Security

Test Objectives

- Perform a test that demonstrates the potential vulnerability of equipment connected to the power grid
  - Only a single scenario and configuration can be tested
- The test will be conducted to confirm the vulnerability and impacts under real-world conditions
  - The system under test must be configured in a way that complies with industry best practices as confirmed by test participants prior to test execution
- Data from the test will be used to validate previous modeling and simulation results, demonstrate and catalog physical consequences, and provide a baseline for future tests

Homeland Security

Pages 24 through 26 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Notable Quotes

"The Aurora project did demonstrate that the ability to exploit the capability of modern protective equipment and cause them to serve as a destructive weapon. I feel that the same results could be achieved by any competent power system protection engineer if provided access and the desire to do so."

Tim Ernst, Utility power system engineer with 25+ years in the industry

"These types of results could be expected if similar operations occurred against a utility or industrial plant."

Ed Terlau, Utility power system engineer with 35+ years in the industry

"With this demonstration... it is clearly time we address the security and integrity of substation devices and protection equipment."

Charles Mozina, Utility power system & generator expert

"Substations represent the most significant information security vulnerability in the power grid."

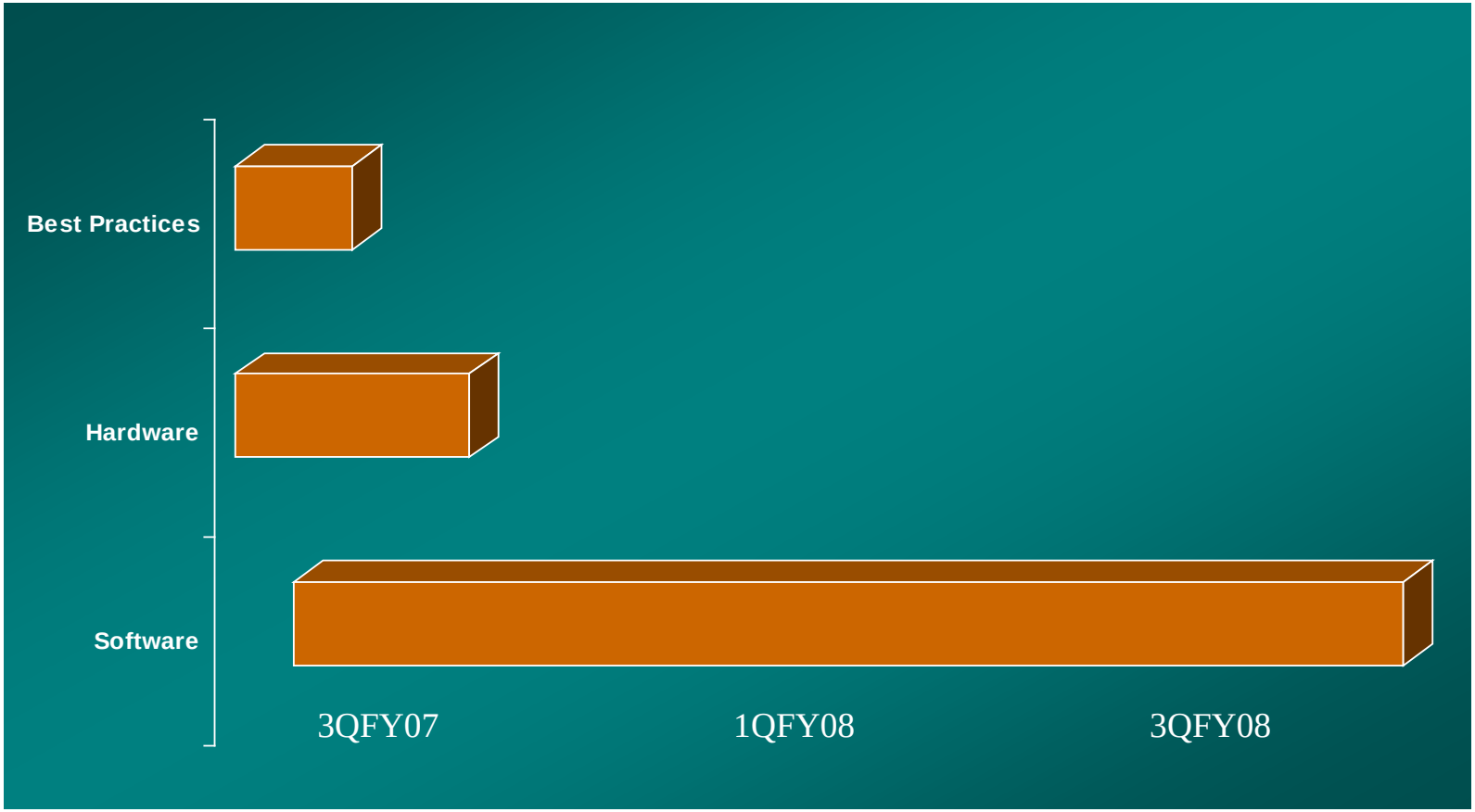
NSTAC Electric Power Risk Assessment 1995

Next Steps

- **<Place Holder>**

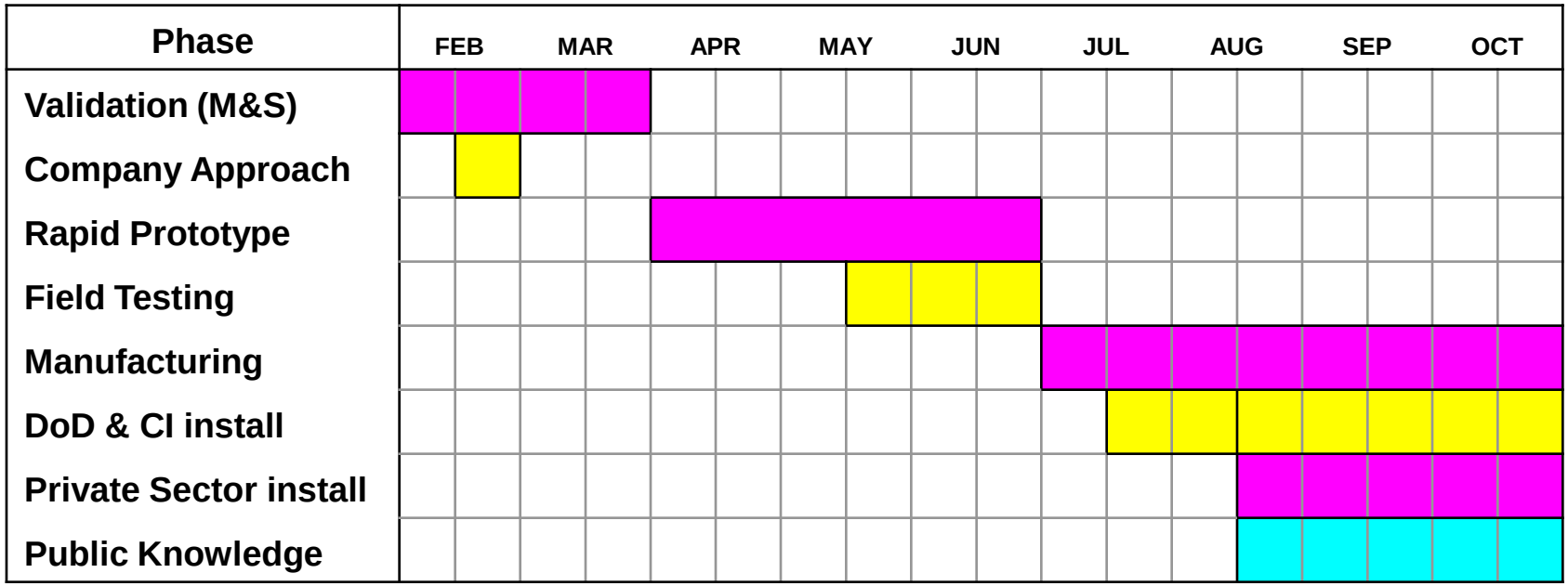
Homeland Security

Mitigation Planning



Homeland Security

Hardware Mitigation Plan/Funding



	Funding Required
Total Funding Required	$1,500K
DHS/Control Systems Security Program	$500K
Unfunded Requirement	$1,000K

Homeland Security

Knowledge Gap Assessment

- **<Place Holder>**

Homeland Security

Control Systems Security: Current Activities

- **<Place Holder>**

Homeland Security

Homeland Security

Test Area Characterization (Physical)

Homeland Security


EXIT
RTDS
RTDS
RTDS

Aurora:
The Power Grid as an Attack Vector

May 7, 2007

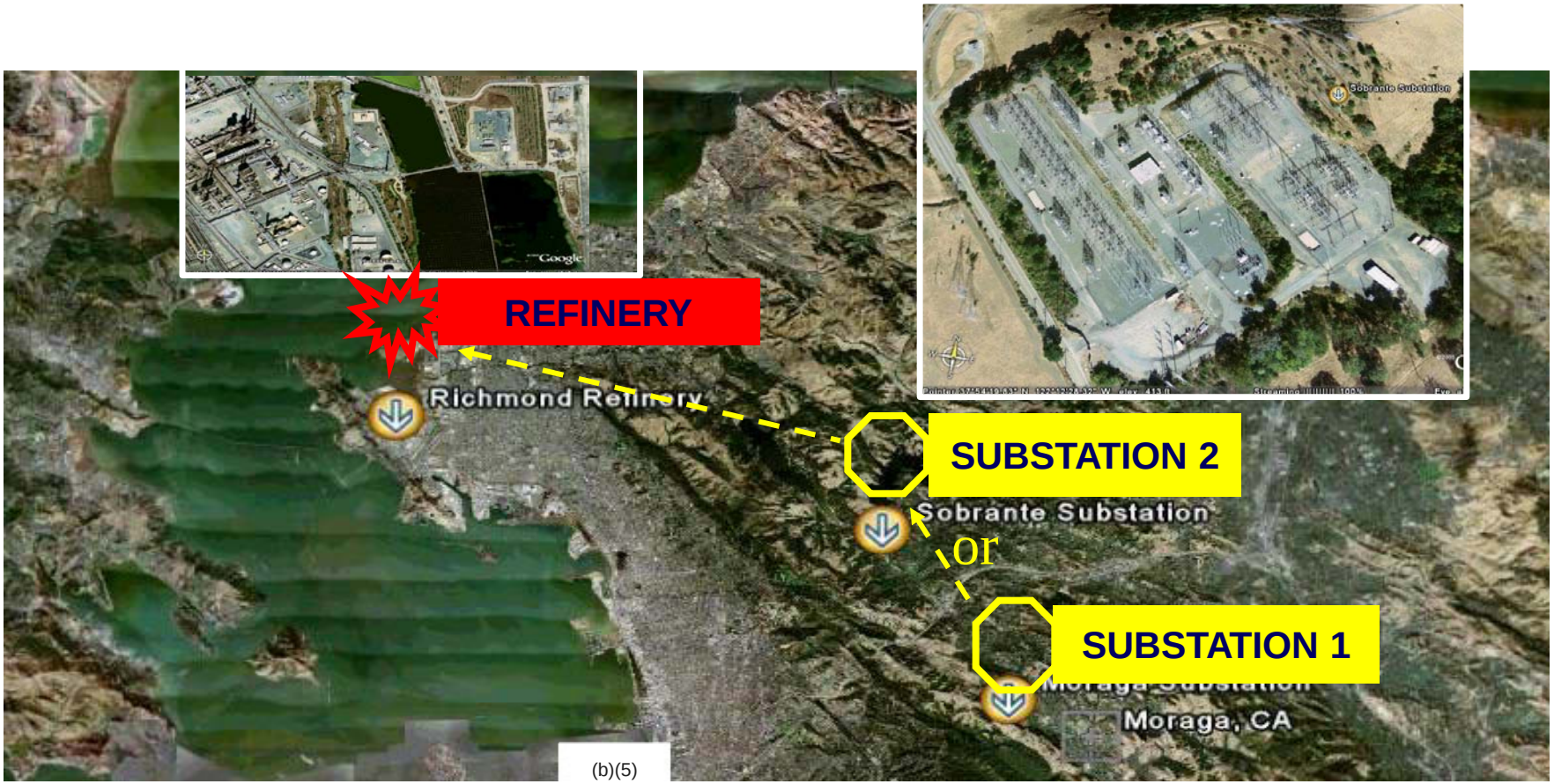
Homeland Security

Agenda

- Executive Summary
- Aurora Vulnerability
- Tiger Team
- Threat Assessment
- Risk Assessment
- Test Preparation and Execution
- Test Team Participants
- Knowledge Gap Assessment
- Mitigation Planning – Next Steps
- Control Systems Security Current Activities

Pages 38 through 41 redacted for the following reasons:
- -
(b)(5), (b)(7)f
(b)(7)f, (b)(5)

Aurora Vulnerability



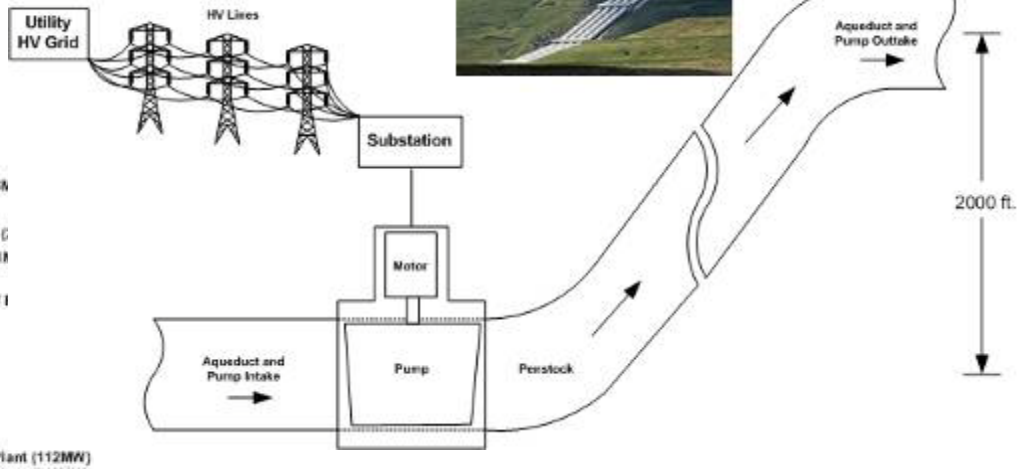
Aurora Vulnerability

Programmable Digital Relay

- The Elements Necessary for an Attack
  - Programmable Digital Relay
    - Or other device that controls the breaker
  - High-Speed Breakers
  - Access (front panel, modem, Internet, wireless, or SCADA)
  - Laptop/Desktop Computer
- Knowledge Necessary:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)
- Time Required to Conduct the Attack (after gaining access):
  - Less than one minute
  - No additional software is introduced
  - Uses the internal settings of the imbedded relay software

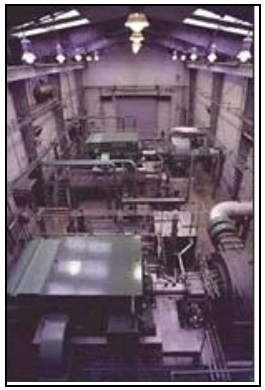
Aurora Vulnerability Example

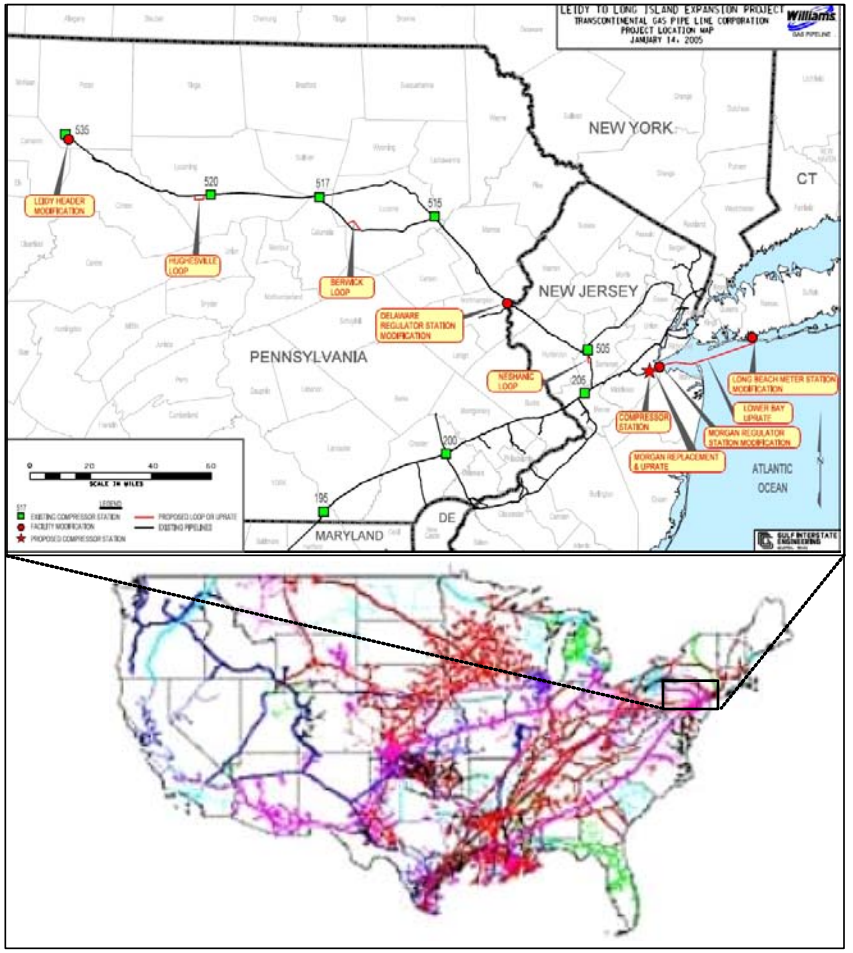
Water Pumping Plants Use Large Motors in Series



Aurora Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities





Page 46 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Tiger Team

- U/S Foresman directed the formation of a Tiger Team to scope the vulnerability, threat, and risk of the Aurora scenario
- Tiger Team response indicated a reason for concern and U/S Foresman established a milestone for a physical test
- Tiger Team was expanded from Federal stakeholders to include representatives from private industry
  - North American Electrical Reliability Corporation
  - Tennessee Valley Authority
  - Electric Sector Coordinating Counsel
- Execute the test and evaluate results quickly then develop mitigation strategy based on the result

Aurora Threat Assessment

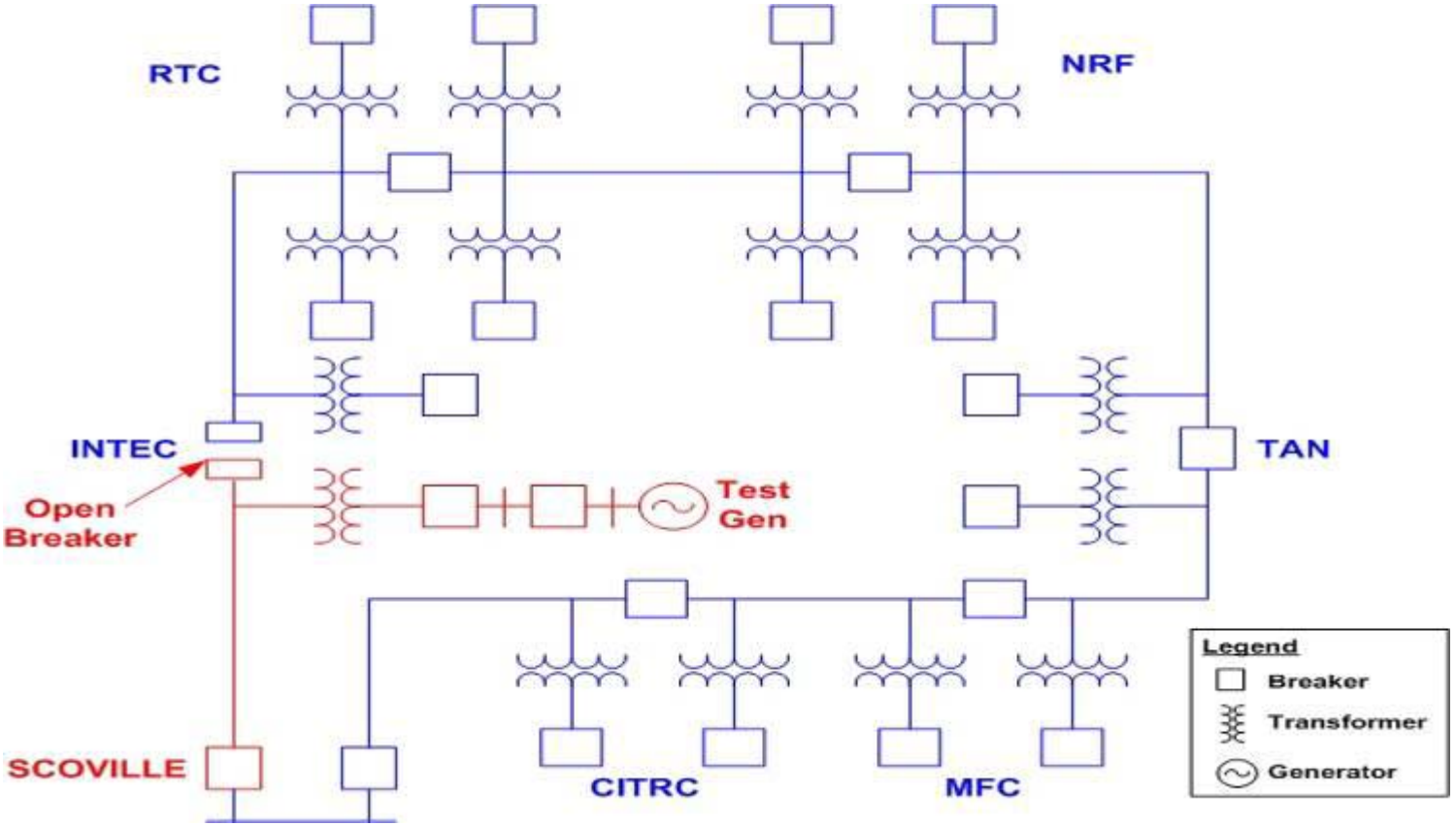
Provided by HITRAC - ~~SECRET~~ Briefing

Aurora Risk Assessment

Provided by IP/RMD - ~~SECRET~~ Briefing

Pages 50 through 52 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Test Area Characterization (Electrical)



The 138 kV Loop Was Configured to Minimize Power Disturbances to the Remainder of INL

Homeland Security

Test Site Prep

Homeland Security

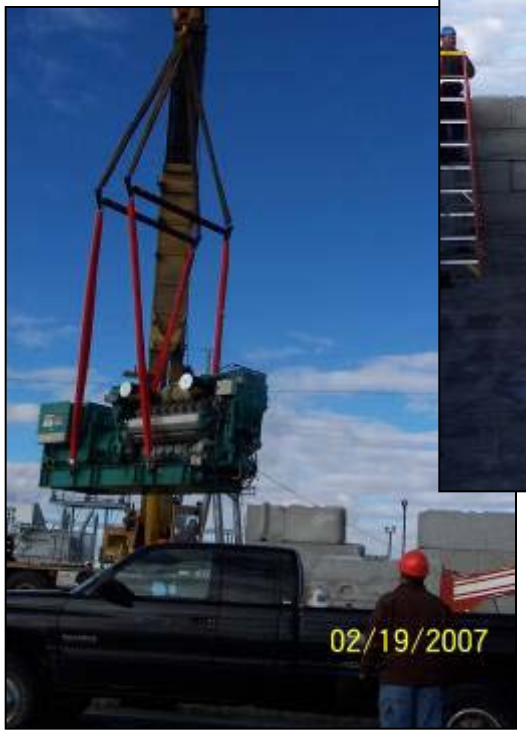
Pouring the Pad

Building the Safety Wall

Homeland Security

Shipping the Generator

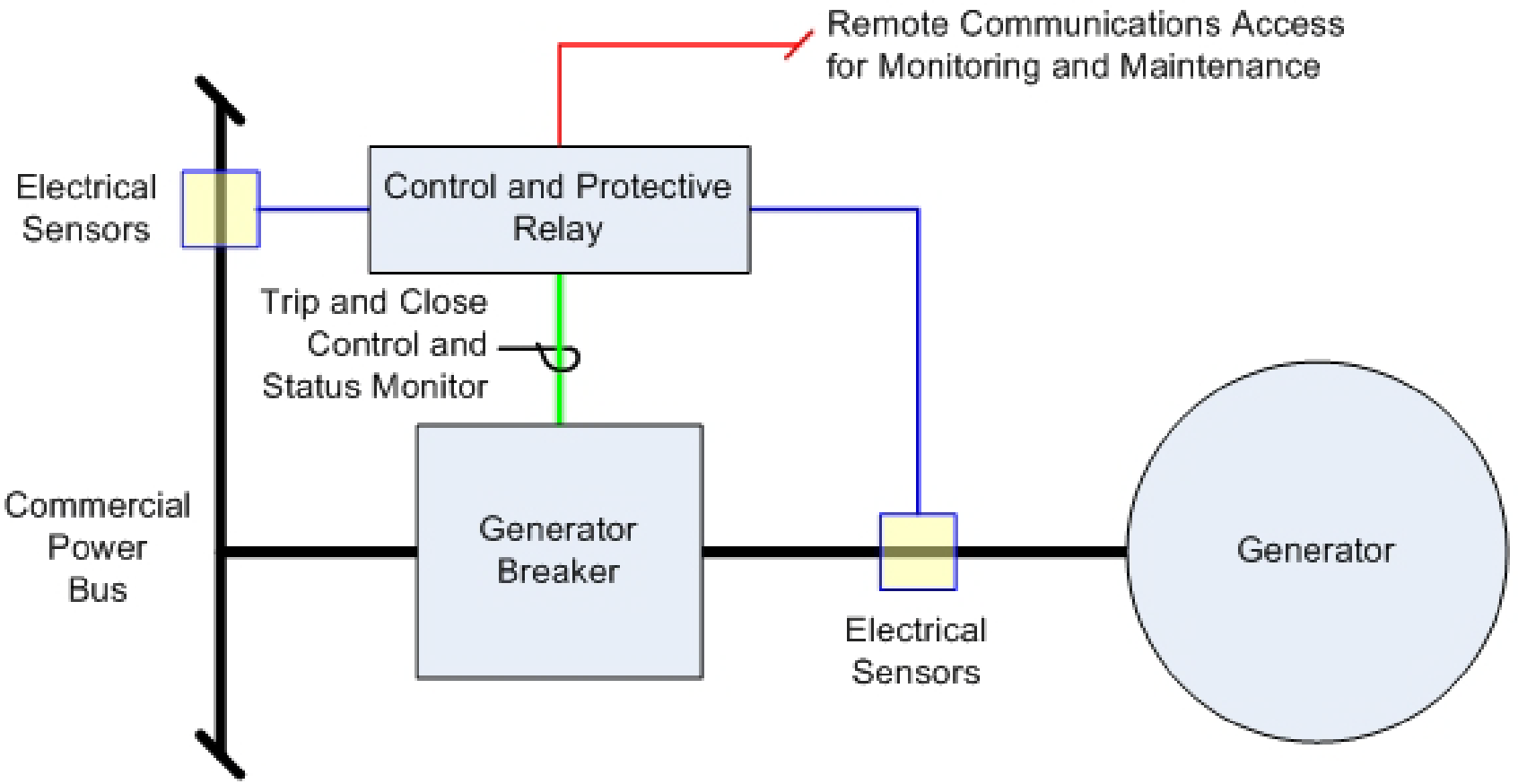
Placing the Generator



Homeland Security

Setup and Configuration

Simplified Control Diagram



Page 61 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Test Team Participants

NAME	ORGANIZATION	ASSIGNED RESPONSIBILITY
(b)(7)f, (b)(4), (b)(6), (b)(7)c		Electrical Engineer
		Protection/Electrical Engineer/Utility
		Generator SME/Electrical Engineering
		Electrical Engineer/Utility
		Control Systems Security
		Utility Operations
		SCADA/Engineering
		Electrical Engineer/Utility
		Electrical Engineer
		Cyber Security Research

Test Team Participants (Cont.)

NAME	ORGANIZATION	ASSIGNED RESPONSIBILITY
(b)(4), (b)(6), (b)(7)c, (b)(7)f		Level IV Division Manager Program/Project Manager Test Director ALD Management Instrumentation Engineering Manager Construction Power Management Planning and Controls Environmental Cost Estimating/Security

Test Team Participants (Cont.)

NAME	ORGANIZATION	ASSIGNED RESPONSIBILITY
(b)(4), (b)(6), (b)(7)c, (b)(7)f		Procurement & Project Engineering Electrical Engineer Electrical Engineering Modeling/Simulation Modeling/Simulation Power Management Operations/ES&H Coordination Engineering/Safety/PEP Quality Quality

Notable Quotes

"The Aurora project did demonstrate that the ability to exploit the capability of modern protective equipment and cause them to serve as a destructive weapon. I feel that the same results could be achieved by any competent power system protection engineer if provided access and the desire to do so."

Tim Ernst, Utility power system engineer with 25+ years in the industry

"These types of results could be expected if similar operations occurred against a utility or industrial plant."

Ed Terlau, Utility power system engineer with 35+ years in the industry

"With this demonstration... it is clearly time we address the security and integrity of substation devices and protection equipment."

Charles Mozina, Utility power system & generator expert

"Substations represent the most significant information security vulnerability in the power grid."

NSTAC Electric Power Risk Assessment 1995

Knowledge Gap Assessment

- Tiger Team will work with industry partners to identify current unknown critical information needed to assess the risk and develop a work plan for risk mitigation:
  - Identify protective relays and other devices that may be susceptible to this exploitation
  - Identify currently installed base of vulnerable relays
  - Identify exposure of this installed equipment to physical and remote access
  - Identify security technologies and procedures currently in place
  - Identify and evaluate applicable standards
  - Determine effectiveness of security technologies and procedures presently installed
  - Determine sensitivity of the scenario parameters
  - Determine susceptibility of rotating equipment damage as a function of distance from the event initiation
  - Conduct an inspection of a statistically relevant number of “protective relays” to determine any type of existing physical or cyber exploitation or compromise

Mitigation – Next Steps

- Greatest potential for exploitation of the vulnerability exists in the electrical sector; concentrating efforts there first
- Tiger Team will work jointly with Industry through the Sector Coordinating Councils (SCC) addressing the following:
  - Identify resources from Private Sector needed to address the knowledge gaps listed on the previous slide.
  - SCCs will establish task groups to work with the Aurora Tiger Team to address the list of knowledge gaps.
  - Clarify the extent of risk associated with the Aurora vulnerability.
  - Develop appropriate, cost-effective mitigation solutions.
  - Leverage multiple venues to disseminate mitigation solutions to ensure engagement of all components of a sector (e.g., trade associations).
- Tiger Team will work with the Electric and Nuclear sectors first, and then reach to other sectors as determined.
- Tiger Team will then reach out to appropriate protective relay vendors to enhance vendor understanding of possible risks associated with the Aurora Vulnerability, to encourage modifications to protective relay functionality, and to facilitate notification to affected industry sectors.

Control Systems Security: Current Activities

- DHS Federal Control Systems Security Working Group is developing the Federal Coordinating Strategy for Securing Control Systems to address cross-sector DHS responsibilities
- DoE through the National SCADA Test Bed and the Roadmap to Secure Control Systems in Energy Sector provide focus and guidance for the Energy Sector
- DHS/DoE perform outreach and awareness to public and private sector through education, training, conferences, seminars, and the promotion of industry recommended practices
- DHS/DoE Performing equipment and systems vulnerability assessments and the supporting tools and technologies
- DoD has provided significant investment in control systems modeling and simulation capability that made much of the Aurora testing and assessment work possible
- DoD partnering with DHS, DoE, and other Federal agencies to protect the critical infrastructure of the Defense Industrial Base
- DHS is working through HITRAC to educate the intelligence community on the indicators and warnings of controls systems and SCADA attack scenarios

Homeland Security

Control Systems Security

Aurora Update Brief

Agenda

- Executive Summary
- Aurora Project Review
- Knowledge Gaps
- Current Status
- Next Steps

Pages 72 through 74 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

Aurora Update Brief

Agenda

- Executive Summary
- Aurora Project Review
- Knowledge Gaps
- Current Status
- Next Steps

Pages 78 through 80 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

Aurora Update Brief

Agenda

- Aurora Project Review
- Technical Team Efforts
- Mitigation Plan - Next Steps

Pages 84 through 86 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

Aurora Update Brief

Agenda

- Aurora Project Review
- Technical Team Efforts
- Mitigation Plan - Next Steps
- Mitigation Plan - Draft

Pages 90 through 94 redacted for the following reasons:
- -
(b)(5), (b)(7)f
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

AURORA Update

June 10, 2007

Homeland Security

Page 97 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Aurora Classification Guidance

- Aurora Classification Guidance is based on the Department of Homeland Security Classification Guide DHS SCG-004-OS (CIP) – Critical Infrastructure Protection for DHS Assets (September 2006), which is based upon Executive Order (EO) 12958, “Classified National Security Information”
- The Aurora Project Team has designated all Aurora related information as “Unclassified, for official use only”
- Aurora information is “Unclassified, for official use only” to ensure successful implementation of the mitigation strategy in partnership with private industry
- Once the Aurora Mitigation Plan has been successfully implemented, other information related to specific critical assets remaining in a vulnerable state will be classified

Mitigation Timeline

- Finalize joint Nuclear and Electric Sectors' mitigation measures (May 16, 2007)
- Address coordination with select vendors on enhanced security measures, without revealing the Aurora vulnerability (May 2007)
- Update of Press Release in case of unintended information release (May 2007)
- Finalize Aurora Mitigation Plan and roll out (May 18, 2007)
- Determine additional sectors for immediate outreach based on risk profile, and conduct outreach as appropriate (May/June 2007)
- Additional briefings to EOP, Congress, GAO (May/June 2007)
- Execution of first phase of Mitigation Strategy (May-July 2007)

Pages 100 through 101 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

AURORA Update

July 9, 2007

Homeland Security

Page 104 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Mitigation Timeline

- Nuclear/Electric Sectors' initiate first phase Mitigation Plan - complete
- Update Canada, United Kingdom, Australia, New Zealand - complete
- Coordinate with vendors on enhanced security measures - complete
- Update Public Affairs Guidance in case of unintended release of information – completed/refreshed every 30 days
- Identify additional sectors for outreach based on risk profile - complete
- Complete first phase field testing of prototype Rotating Equipment Isolation Device (REID) to meet DoD requirement (7/2007)
- Initial production run of REID device (8/2007) with initial devices employed by DoD OCONUS
- Significant vulnerability reduction to critical infrastructure expected within the first 60 days

Recent Activity

- Public Affairs Guidance updated and coordinated with DOE, FERC, NRC, NERC, DoD, and the Electric/Nuclear Sectors
- NERC released ES-ISAC Advisory on the Aurora vulnerability to include the mitigation plan
- Updated the House HSC members and Senate HSGAC staff
- Provided the first briefing to the EMP Commission
- Briefed the JASON study group on Aurora as they prepare a report to DHS S&T on R&D directions
- Based on primary concern of large and difficult to replace rotating equipment continue reach out to other sectors

Pages 107 through 108 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Aurora Classification Guidance

- Aurora Classification Guidance is based on the Department of Homeland Security Classification Guide DHS SCG-004-OS (CIP) – Critical Infrastructure Protection for DHS Assets (6/2006), which is based upon Executive Order (EO) 12958, “Classified National Security Information”
- Draft Classification Guidance is being staffed with Core Interagency team members and DHS security
- The Aurora Project Team has designated all Aurora related information as “Unclassified, for official use only”
- Aurora information is “Unclassified, For Official Use Only” to allow for successful implementation of the mitigation strategy in partnership with private industry
- Once the Aurora Mitigation Plan has been successfully implemented, information related to specific critical assets remaining in a vulnerable state will be classified

Homeland Security

Control Systems Security

AURORA Update

Page 112 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Aurora Classification Guidance

- Aurora Classification Guidance is based on the Department of Homeland Security Classification Guide DHS SCG-004-OS (CIP) – Critical Infrastructure Protection for DHS Assets (September 2006), which is based upon Executive Order (EO) 12958, “Classified National Security Information”
- The Aurora Project Team has designated all Aurora related information as “Unclassified, for official use only”
- Aurora information is “Unclassified, for official use only” to ensure successful implementation of the mitigation strategy in partnership with private industry
- Once the Aurora Mitigation Plan has been successfully implemented, information related to specific critical assets remaining in a vulnerable state will be classified

Mitigation Timeline

- Nuclear/Electric Sectors' initiate first phase Mitigation Plan (June 20, 2007)
- Update with Canada, United Kingdom, Australia, New Zealand (June 2007)
- Coordinate with select vendors on enhanced security measures (June 2007)
- Continuously update Public Affairs Guidance in case of unintended release of information
- Identify additional sectors for immediate outreach based on risk profile (June/July 2007)
- Complete field testing of prototype Rotating Equipment Isolation Device (REID) (July 2007)
- Initial production run of REID device (August 2007)

Page 115 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

AURORA Update

Page 118 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)f, (b)(5)

Aurora Classification Guidance

- Aurora Classification Guidance is based on the Department of Homeland Security Classification Guide DHS SCG-004-OS (CIP) – Critical Infrastructure Protection for DHS Assets (September 2006), which is based upon Executive Order (EO) 12958, “Classified National Security Information”
- The Aurora Project Team has designated all Aurora related information as “Unclassified, for official use only”
- Aurora information is “Unclassified, for official use only” to ensure successful implementation of the mitigation strategy in partnership with private industry
- Once the Aurora Mitigation Plan has been successfully implemented, information related to specific critical assets remaining in a vulnerable state will be classified

Mitigation Timeline

- Nuclear/Electric Sectors' initiate first phase Mitigation Plan (June 20, 2007)
- Update with Canada, United Kingdom, Australia, New Zealand (June 2007)
- Coordinate with select vendors on enhanced security measures (June 2007)
- Continuously update Public Affairs Guidance in case of unintended release of information
- Identify additional sectors for immediate outreach based on risk profile (June/July 2007)
- Complete field testing of prototype Rotating Equipment Isolation Device (REID) (July 2007)
- Initial production run of REID device (August 2007)

Page 121 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Homeland Security

Control Systems Security

AURORA Update

Page 124 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Aurora Classification Guidance

- Aurora Classification Guidance is based on the Department of Homeland Security Classification Guide DHS SCG-004-OS (CIP) – Critical Infrastructure Protection for DHS Assets (September 2006), which is based upon Executive Order (EO) 12958, “Classified National Security Information”
- The Aurora Project Team has designated all Aurora related information as “Unclassified, for official use only”
- Aurora information is “Unclassified, For Official Use Only” to ensure successful implementation of the mitigation strategy in partnership with private industry
- Once the Aurora Mitigation Plan has been successfully implemented, information related to specific critical assets remaining in a vulnerable state will be classified

Mitigation Timeline

- Nuclear/Electric Sectors' initiate first phase Mitigation Plan (June 20, 2007)
- Update with Canada, United Kingdom, Australia, New Zealand (June 2007)
- Coordinate with select vendors on enhanced security measures (June 2007)
- Continuously update Public Affairs Guidance in case of unintended release of information
- Identify additional sectors for immediate outreach based on risk profile (June/July 2007)
- Complete field testing of prototype Rotating Equipment Isolation Device (REID) (July 2007)
- Initial production run of REID device (August 2007)

Page 127 redacted for the following reason:
- -
(b)(7)f, (b)(5)

Homeland Security

Pages 129 through 132 redacted for the following reasons:
- -
(b)(7)f, (b)(5)

Pages 144 through 170 redacted for the following reasons:
- -

Control Systems Security Center
Weekly Accomplishments and Activities

Week Ending 10/26/2007

1.0 OUTREACH AND AWARENESS

- Sent the OPSEC on line training out to selected members of industry for review and comment. The review period is from October 23-November. Comments received to date are positive. After the industry review period, all of the comments will be collated and evaluated for inclusion or modification of the on-line OPSEC training.
- Participated in the Meridian conference in Stockholm Sweden. CSSP provided a presentation on control systems security and led a panel discussion. Hun Kim also attended the conference and spoke about the role of government and the interactions or partnerships with industry that need to be entreated.

2.0 RISK REDUCTION

- Received the comments on the "Cross-Site Scripting" and "Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments" recommended practices. The comments have been incorporated, and re-submitted to NCSD for final approval.
- Further development work on the Forensic, Incident Response, and Configuration Management recommended practices were completed this week.
- New future topics for the Procurement Language document are also under development.
- Completed the final checkout for CS^2SAT delivery to ISA. BEA attorneys have reviewed and approved the ISA End User License Agreement that is included in the application software. Still waiting for approval on the main BEA/ISA licensing contract.
- A proposed delivery package including whitepaper, introductory letter, and a brief explanation of the CS^2SAT for government users has been prepared and delivered to DHS. Still waiting for approval on the government End User License Agreement before the package can be assembled for delivery to the US Army Corp of Engineers.

3.0 TECHNOLOGY ASSESSMENT

- The third validation assessment on the Firmware Upgrade vulnerability document was completed and delivered to NCSD. Further discussions of disclosure of information will be held next week.

- The combined Firmware Upgrade Vulnerability report is getting close to completion. A draft copy will be available next week for review. The final validation test has been incorporated this week.
- Completed the Adventium Labs system setup and began assessment activities. Due to the restrictions of the system, the assessment activities will be limited.
- The Teltone assessment work continues with TOE evaluations.
- Developed a point paper on Industrial defender and had negotiations on the Industrial defender product procurement.

4.0 CYBER METRICS AND ANALYSIS

- The prototype firewall rule analyzer from Mouna Seri of the University of Illinois has been installed and now executes. Logistics are being worked out to determine if the analyzer can actually run on the power substation control network in order to automatically acquire the firewall rules.
- Metrics for the SCADA test case are being calculated based on the data collected. A few of the metrics need more data to be collected at the site. The additional data collection is scheduled to take place November.
- Review of seven previous vulnerability assessments to identify the vulnerabilities, recommended mitigations, and their possible impact on the proposed metrics has been completed. 410 findings and recommendations are still undergoing evaluation and mapping to the proposed technical metrics and ideals. Summary rollups will be created. All of this work will be documented and used in a paper for S4 and for the final Metrics report.
- The scenario development task continues. A variety of books and documents have been reviewed and a decision was made to have the initial attack come through a Genco's corporate network, into the control room, with a compromise of the ICCP server communicating with the ISO's ICCP server. Writing of a draft document for this initial stage of the attack will commence next week.

5.0 DEVELOP PARTNERSHIPS

- Issued the Vendor Forum minutes for the October 9 conference call. The subjects discussed during the call included a proposed charter for the Vendor Forum and the mitigation actions that DHS has taken in response to the Aurora project. The vendor forum is considering meeting at the SANS Control Systems and SCADA Security Summit in New Orleans, January 2008 to discuss the Charter.

6.0 US-CERT OPERATIONS SUPPORT

- Completed a Weekly Digest of the incidents, events, and CVEs for the week and posted to the secure portal.
- The Quarterly report (July-September 2007) is in final editing and internal review to be issued to CSSP PMO next week.

- A summary of US-CERT support activities is being prepared for a meeting between Vishant Shah and Mike Witt, acting director US-CERT next week.
- The weekly phone call with the US-CERT CSSA and with LLNL was conducted with no information to report.

7.0 NCSD COORDINATION

- No activity to report.

8.0 PROGRAM MANAGEMENT

- Conducted the Lab Leadership Meeting in Washington, DC.

UPCOMING ACTIVITIES AND EVENTS

- November 6-7 – API 2nd Annual IT Security Conference, Houston, Texas. (b)(6) (b)(6) is planning to attend. The I^3P will also be providing a pre-conference training on November 5.
- November 13 – Vendor Forum Conference call

Control Systems Security Center
Weekly Accomplishments and Activities

Week Ending 11/09/2007

1.0 OUTREACH AND AWARENESS

- The OPSEC on-line training course industry review period was completed on November 5, and the development web site was taken down. An invitation to review the OPSEC on-line training was sent to approximately 125 people in industry, of which 71 people logged into the training. The industry and internal review resulted in 173 comments from 28 different people. PNNL starting working on the modifications to the training, in preparation for NCSD approval.
- Held conference call with Shell Oil Company in The Netherlands. The purpose of this conference call was to discuss: 1) How Shell should use the training with their Fountains system, 2) Identify the best way for Shell to provide input to the content of the training, and 3) Proposed time frame. Shell Oil Company is interested in having their engineers and operators, and potentially other staff take the NCSD on-line training.
- Participated in the SANS Process Control and SCADA Security Summit planning conference call. DHS announced that NCSD will sponsor control systems training at the event at no cost to the attendee. The training courses as currently planned for include the 4-hour introduction to control systems security, the 8-hour hands-on Intermediate Control Systems Security and the 8-hour Control Systems Security for IT Professionals.
- **Actions – Decisions Needed**
  - Will PCSF working groups be meeting prior to the SANS conference
  - International advanced training week after PCSF

2.0 RISK REDUCTION

- Incorporated the CSSP PMO comments on the "Securing Control System Modems" recommended practice and re-submitted to the CSSP PMO for final approval. Work also continues on the incorporation of comments from the CSSP PMO on the "Hardening Guidelines for OPC Hosts," along with the two supporting OPC documents. These should be completed and delivered next week.
- Final approval was obtained on the "Cross-Site Scripting" recommended practice and the web site has been prepared for the re-posting of the approved document. Information on the web site posting will be completed next week.
- The next version of the Procurement Language is under development with new topic areas in remote access (serial, VPN, Web, TCP/IP), Network partitioning, and physical

security. The draft copy will be ready for technical editing in late November and the version will be finalized for posting and publication for the SANS Summit in January.

- The "Incident Response" recommended practice is being developed by the Matrikon subcontractor. Coordination efforts with the US-CERT Incident Response will be incorporated into the document.
- Participated in the weekly SAT call and discussed the status of the review of NIST SP800-82.
- (b)(6) participated in the ISA 99 WG4 conference call. The new SharePoint web site was demonstrated and discussed. A discussion on security levels followed.
- Drafted an abstract for a paper based on the CoR to be presented at an ISA symposium.
- Finished a draft of the revision of the Sector Summary report. Coordinating Councils information is one key addition.
- (b)(6) (Argonne National Laboratory) discussed the status of natural gas industry feedback on the CoR with (b)(6) (b)(6) and (b)(6) (b)(6) during a teleconference related to an NSTB activity. (b)(6) is interested in reviewing the CoR requirements and their applicability in developing natural gas-specific SCADA security standards as a part of an INGAA SCADA Security Workshop in late January 2008. Argonne has been asked to assist and a follow up discussion is planned.
- Delivered copies of CS^{2}SAT version 1.0.0 for the government to USACE. This completes the cooperative WFO project with USACE to incorporate DoD Directive 8500.2 into the tool. Still waiting for address confirmation on the appropriate USACE Headquarters contact for a summation letter.
- Continued discussions with (b)(6) of the Vulnerability Assessment Group, an Australian company specializing in cyber assessments, on the possibility of a cooperative development agreement to improve the Security Assurance Level component of the CS^{2}SAT.

3.0 TECHNOLOGY ASSESSMENT

- Industrial Defender procurement was approved and scheduling for the setup and configuration of the system is being planned for the end of November for product evaluation in December. This product will also be used for assessment activities and partnering opportunities with security expert in the public sector.
- Completed the consolidated Firmware Upgrade Vulnerability draft report. Internal review will be conducted next week in preparation for the briefing to NCSD.
- Completed the Adventium Labs system assessment activities and a report is currently being developed. This assessment was terminated early due to significant findings and the state of the system. Details will be contained within the report. The technology has high potential but is not ready for production.
- Work continues on the Teltone Corporation assessment.

- The new version of the ABB 800xa system was received this week, setup and configured by ABB. Assessment activities are continuing.

4.0 CYBER METRICS AND ANALYSIS

- The prototype firewall rule analyzer from Mouna Seri of the University of Illinois has been modified and returned. This modification makes the tool more useful for calculating the proposed reachability metric.
- The case study of metrics for an electric power substation SCADA is continuing. All the data needed to complete the study has been obtained. The data is now being analyzed and documented for the final report.
- Began drafting the Technical Metrics Final Report.
- Metrics validation analysis (comparison of assessment findings with proposed ideals and metrics) write-up is underway for inclusion in the S4 paper and the final metrics report. All findings and recommendations were found to match, to a varying degree, with the proposed security ideals. Charts displaying the analysis have been completed and included in the write up. Recommendations to drop, add, or alter metrics are being formulated based on these results.
- Scenario development involving the compromise of the grid's market mechanisms via a SCADA control room attack is proceeding. Significant sections are being developed and documented. The market side is just beginning to be understood enough to flesh out the final steps in an attack and the plausible high level consequences.
- Analysis support is being provided to the firmware vulnerability task. A hypothetical example scenario is being developed to provide a sense of the possible consequences.

5.0 DEVELOP PARTNERSHIPS

- Issued the Vendor Forum minutes for the September conference call. Mark Hadley (PNNL) was the guest speaker and the subject was the "Catalog of Control Systems Security: Recommendations for Standards Developers."
- Working to issue a contract with Noblis to support the SANS and PCSF events. The terms of the contract are being negotiated and discussed between the INL and Noblis attorneys.
- Issued agenda for the Vendor Forum conference call. The conference call is scheduled for November 13, 2007. The agenda includes discussing the CS^2SAT license with ISA, a heads-up that DHS will be developing a national strategy and will be looking for their support and input, and discussion of the Vendor Forum charter.

6.0 US-CERT OPERATIONS SUPPORT

- Completed a Weekly Digest of the incidents, events, and CVEs for the week and posted to the secure portal.
- The Quarterly report (July-September 2007) has been posted to the secure portal.

- Discussions with Team Cymru were held to firm up a visit to INL on December 6. Their company is collaborating with INL in the collection and analysis of data to identify indicators of malware targeting critical infrastructure control systems. They will present capabilities and discuss opportunities to support CSSP.
- A weekly status call for US-CERT operational awareness was held with (b)(6)

(b)(6)

7.0 NCSD COORDINATION

- No activity to report.
- **Actions – Decisions Needed**
  - Need scope defined and plan of action for the National Strategy development

8.0 PROGRAM MANAGEMENT

- Updated the FY-08 Prioritized List and worked with NCSD to draft the FY-08 Statement of Work.

UPCOMING ACTIVITIES AND EVENTS

- November 13 – Vendor Forum Conference call
- November 20 – (b)(6) representing DHS CSSP will be visiting INL to discuss the Aurora project.

Control Systems Security Center
Weekly Accomplishments and Activities

Week Ending 11/30/2007

1.0 OUTREACH AND AWARENESS

- Working on developing a contract with SANS to provide logistics support, advertising, and registration for the training courses and PCSF working group meetings prior to the SANS Process Control and SCADA Security Summit on January 16-17.
- Developed and issued a Dashboard for the SANS Process Control and SCADA Security Summit. This will be updated weekly.
- Submitted the OPSEC on-line training course for CSSP PMO review and approval. The request for review and approval was accompanied by a one page overview.
- Developed the quarterly website report and forwarded to CSSP PMO.
- **Actions – Decisions Needed**
  - Comments on the OPSEC for Control Systems on-line training is requested by December 12, 2007.

2.0 RISK REDUCTION

- The Matrikon subcontractor has submitted the draft "Incident Response" recommended practice. The document was submitted for the first round of industry reviews. The review cycle is two weeks with comments due back by December 13.
- Partnered with LoftyPerch personnel to draft the "Forensics for Control Systems" recommended practices. Development work continues.
- Development work on the "Configuration Management" recommended practices continues.
- Conducted a quick review of the seven SCADA Security Good Practice Guides for CPN1 (formerly NISCC). The SCADA Security Good Practices are currently linked to the Recommended Practices website. The review consisted of subcontractors and internal personnel with the expertise and background on the topics. Comments were submitted to the CPN1 on November 30, 2007.
- The new version of the Procurement Language for Control Systems is nearing completion. Four new topics areas were added. This document is scheduled to be delivered to Will Pelgrin by December 7 for review.
- In response to DHS PMO latest comments, the SAT updated the Catalog of Control System Security: Recommendations for Standards Developers and sent it to the CSSP PMO.

- Wayne Manges reported the following: "The ISA100 team has renewed its emphasis on improved security with the rebirth of the Security Working Group. The ISA100 meeting in Houston in October 2007 launched new focus on a number of interest groups including discrete manufacturing, distribution automation, and asset management along with improved security. The security group, after input from Scott Mix (NERC) and others, was reconstituted as the "Trustworthy Wireless Interest Group" so that security and reliability could be considered together. The group (with Scott Mix and Wayne Manges as co-chairs) has now had several telephone meetings and is planning its first face-to-face meeting in Richmond, Virginia (hosted by ExxonMobil) in January 2008. The first deliverable is tentatively scheduled to be a document with the working title of "The Technology of Trustworthy Wireless for Industrial Automation." The group has direct representation and collaboration with the ISA99 standards body with cross members active in both groups."
- Completed development and testing of CS^2SAT version 1.0.1 and shipped to ISA and the USACE. This version corrected a few minor problems uncovered by ISA.
- Dave Kuipers, INL NSTB Program Manager, passed along a request from Hank Kenchington of DOE-OE, expressing an interest in a cooperative effort to include Oil and Natural Gas sector specific content into the CS^2SAT. CSSP has the action to review the available standards in those sectors and to develop preliminary recommendations and costs.

3.0 TECHNOLOGY ASSESSMENT

- The consolidated Firmware Upgrade Vulnerability report was completed with all the internal comments incorporated. The report has been submitted for technical editing and will be submitted next week to management one-over reviews prior to submission to the CSSP PMO.
- Contacted vendor on the Firmware vulnerability and established a sit down disclosure meeting on December 12, 2007.
- Adventium Labs system assessment report has been completed and submitted for technical editing. The report was submitted this week for management one-over reviews. Estimated delivery of the second assessment report is December 14.
- Work continued on the Teltone assessment this week. The assessment activities will be completed by next week. The report development has begun and the draft will be completed by December 15.
- The ABB 800xa assessment activities continue.

4.0 CYBER METRICS AND ANALYSIS

- Customer feedback on the INL electric power substation SCADA metrics case study was positive. They also plan to make several changes to their operations as a result of the recommendations in the study. This report will be included as an appendix to the final Technical Metrics report.

- The final set of core technical metrics was chosen after a full day of discussions. Some of the metrics in the original proposed metrics set were deleted, one was added and some were renamed to better reflect the nature of the metrics. Some of the metrics definitions were also refined to clarify how the data would be collected. This final set is the result of two case studies, and seven security assessment evaluations. This final set of metrics will be included in the final Technical Metrics report and in the S4 conference paper.
- The paper for S4 entitled "Measurable Control System Security through Ideal-Driven Technical Metrics" was completed. The paper is now undergoing internal review.
- Scenario development involving the compromise of the grid's market mechanisms via a SCADA control room attack is preceding along with weekly teleconferences with the PNNL collaborators.
- A draft of the white paper exploring economic incentives was completed.

5.0 DEVELOP PARTNERSHIPS

- Issued minutes from the Vendor Forum conference call held on November 13, 2007.

6.0 US-CERT OPERATIONS SUPPORT

- Completed review and accepted NCSD comments on the white paper on a "Cyber Response to Physical Security Breaches for US-CERT" publication as a Technical Information Product (TIP) to be posted on the US-CERT website. A teaser was written and submitted to post to the CSSP website. A link to the US-CERT page hosting the document from the CSSP site will be included in the teaser.
- Developed and posted the Weekly Digest for an analysis of weekly Common Vulnerabilities and Exposures, published incidents, blog sites, and industry contracts.
- Received and responded to a Request for Information (RFI) 948 from US-CERT. A reply was provided for review and forward to NICC.
- Classification guidance for the CSSP was distributed to laboratory membership of the leadership group.

7.0 NCSD COORDINATION

- Participated in the call between the CSSP PMO, SNL and Energetics on developing the Control Systems National Strategy. Will continue to coordinate with all parties in developing the scope, schedule and budget.

8.0 PROGRAM MANAGEMENT

- Drafted the first version of the FY-08 Task Plans and forwarded to CSSP PMO for review. Held a video telephone conference with CSSP PMO to review each work package and highlight potential new activities to be considered in FY-08.

UPCOMING ACTIVITIES AND EVENTS

- December 4 – DHS, SNL, DoD, and DOE visiting INL to discuss the Aurora project.
- December 4-5 – Cyber Storm II planning meeting in Washington DC.
- December 5 – CSSP (b)(6) will be participating in a webcast, sponsored by Control Engineering magazine. Other speakers on this one hour webcast include:

  (b)(6)

- December 5 – CSSP (b)(6) will be providing an 8 hour training, *Control Systems Security for the IT Professional*, to the US Secret Service in Pittsburg, Pennsylvania.
- December 12 – CSSP (b)(6) will be meeting with ABB management to discuss a specific vulnerability.
- December 17-21 – (b)(6) n assignment at the CSSP PMO in Arlington, Virginia.

CSSP Talking Points for SI All-Hands 6-21-07

- CSSP Management Items

- Outreach
  - This week we met with a NCSD/Education and Training Representative to discuss strategy to coordinate Control Systems Security Training among Federal Partners.

- Aurora
  - NERC letter announcing Vulnerability & mitigation
  - The ES-ISAC would publish a vulnerability advisory on 20 June
  - Outreach telecom to vendors – Feedback from vendor is that vulnerabilities are global issues and the vendor community is the only organization that can address this needed.
  - Approval from tiger team to reach out to vendors to discuss vulnerability and mitigation.
  - CSSP Director will follow up internally to get vendors information as soon as possible
  - Once notification is issued, DHS CSSP will provide an email to the vendor community.
  - CSSP will schedule a follow on conference call once the vulnerability note is released (potentially Thursday or Friday of this week)

- US-CERT
  - Coordinating with HITRAC for increased Intel awareness relating to Aurora Project.
  - Providing cyber situational awareness briefing to Chemical Industry HITRAC bi-weekly briefing on behalf of US-CERT
  - Coordinating upcoming July 10th Control Systems Malware meeting

- Piloting of Self-Assessment Tool
  - We continue working on licensing the beta version of the CS^2SAT self assessment tool.
    - Instrument Society of America (ISA) has expressed interest in distributing the tool
    - The CS^2SAT self assessment tool will be presented at the Special interactive, hands-on control system cyber security workshop on 27 June 2007 in Toronto Canada.

- PCSF
  - Stop work order was issued on May 15th to Noblis. OPP received PR on June 18th. Best estimate is process for completion will take at least 30 days.

- Attended Conferences/Meetings

- On June 19th the CSSP provided control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.
- On June 12th the CSSP hosted the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 12th the CSSP provide 4 different control systems cyber security training sessions: a 4-hr training, Cyber Security- Who needs it, How to secure is your Process Control System? Tutorial on CS^2SAT, and Cyber Security Best Practices at the Siemens User Group conference in Orlando, FL. 4-hour training,
- On June 12th, CSSP staff attended the 2007: FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.
- On June 13th the CSSP staff gave a 45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho.

- Upcoming events next week
  - Next week the CSSP will provide:
    - Control systems cyber security training on June 25 entitled, "Control Systems Cyber Security - Who Needs It?" and demonstrates the Control System Self Assessment Tool (CS2SAT) at the American Water Works Association conference (AWWA-ACE) in Toronto, Ontario, Canada.
    - Control systems cyber security training on June 25 entitled "Introduction to Control Systems for IT Professionals," at the GFIRST National Conference in Orlando, Florida. The United States Computer Emergency Readiness Team (US-CERT) Operations staff and Federal Partners received this same training on May 21-22.
    - Control systems cyber security training entitled "Solutions for Process Control Security," and demonstrate the Control System Self Assessment Tool (CS2SAT), at the New Zealand SCADA Security Workshop in Wellington, New Zealand, on June 25-27. This will be the end of a month-long outreach trip in Australia and New Zealand to meet with government agency officials, discuss potential opportunities for future collaborative work, and explore alignment of activities between programs.
    - Presentation on the topic of the National Institute of Standards and Technology (NIST) Special Publication 800-53, the *Catalog of Security Requirements* (draft), and the *Cyber Security Procurement Language for Control Systems* (draft) document to the Special Publication 99 Working Group 4 meeting in Scottsdale, AZ on

June 25. The Instrumentation, Systems, and Automation Society sponsors the SP99 standard, which defines procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance.

- The next monthly Control Systems Cyber Security Vendors Forum teleconference is on July 10th.

CSSP Talking Points for SI All-Hands 7-18-07

- CSSP Management Items
  - Coordinated with (b)(6) on Catalog of Requirements document. Draft document was provided to ISA (Instrumentation, Systems, and Automation Society) SP 99 working group 4 for review and comment.
  - Met with (b)(6) to discuss education and training strategy. The curriculum develop has received positive feedback and is getting used by academia.
  - Met with TSWG (Technical Support Working Group) to discuss new requirement for training gap analysis. CSSP is currently reviewing a TSWG SOW that would be used in a future training announcement.
  - Updating CSSP Program Plan
  - Status of PCSF contract support??
  - New CSSA

- Outreach
  - Rev 1.6 of the Procurement Specification effort (this is now posted on the MS—ISAC web site.
  - We are in discussions with SANS for the next SCADA Summit. Schedule is not yet finalized, but we are thinking that this will be early CY08.
  - Will be meeting with (b)(6) on Thursday to discuss collaboration and leveraging of efforts with Australians.
  - Held vendor monthly phone call and included a presentation by CIP CS (b)(6) on Sector Specific Plans (SSP) and the role of cyber security within these plans.
  - Posted new recommended practice on using 802.11i.
- Aurora (not sure (b)(6) will want to brief all this detail at the all hands. I believe he will simply boil it down to three things: Conducted numerous briefings including Chertoff, Congress, and GAO; Electricity and Nuclear sectors fully engaged with mitigation efforts; Currently engaging other sectors including Dam, Oil & Gas, & ?)
  - 6-25-07 Dam sector presentation and discussion (NCSD/IP hosting)
  - 6-26-07 Briefed the Electromagnetic Pulse (EMP) Commission (HSC/NCSD)
  - 6-26-07 Via VTC briefed Australian critical infrastructure sector leads (NCSD/IP)
  - 6-28-07 Provided GAO with an update on the Aurora project (NCSD)
  - 6-28-07 Update brief to the Senate Homeland Security and Governmental Affairs Committee staff (CS&C/NCSD/OLA)
  - 7-2-07 Briefed the JASON study group
  - Perry provided 3 briefs to FERC on Aurora (7-6-07, 7-10, & 7-11)
  - 7-6-07 Briefed Air Force Under Secretary Sega
  - Cheri McGuire provided an update on Aurora to Secretary Chertoff (7-9-07)
  - 7-11-07 Held a meeting with DHS security on classification guidance
  - 7-11-07 Received initial inputs from Dams/Hydroelectric industry on tailoring the annex to their Sub-sector

- 7-13-07 Status of Mitigation Efforts/Upcoming Events
  - Nuclear Sector provides weekly updates and is making progress in identifying where and to what degree to apply mitigation efforts (detailed scoping)
  - Electric Sector will provide an update by 7-20-07
  - Oil & Gas and Chemical outreach meeting scheduled for 7-17-07
  - Additional FERC briefing scheduled for 7-17-07
  - Water sector meeting is being rescheduled
  - The prototype Rotating Equipment Isolation Device (REID) is being filed tested in partnership with Constellation Energy

- US-CERT
  - New CSSA on board, (b)(6) This week traveling to CSSC for orientation visit.
  - CSSC representatives met last week (July 10th) with US-CERT Management to provide update on Control Systems Malware initiative.
  - Coordinated Focused Operations briefing for SI Branch leadership.

- Piloting of Self-Assessment Tool
  - We continue working on licensing the beta version of the CS^{2}SAT self assessment tool.
    - Instrumentation, Systems, and Automation Society (ISA) has expressed interest in distributing the tool
    - The CS^{2}SAT self assessment tool was presented at the Special interactive, hands-on control system cyber security workshop on 27 June 2007 in Toronto Canada.

- PCSF
  - Stop work order was issued on May 15th to Noblis. OPP received PR on June 18th. Best estimate is process for completion will take at least 30 days.

- Attended Conferences/Meetings
  - On July 12th CSSP participated in a Kick-Off meeting for SCADA Cyber Attack Alert Tool at TSWG. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.
  - On July 2nd the CSSP Director, (b)(6) participated in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

- On June 25th the CSSP provided control systems cyber security training, "Control Systems Cyber Security - Who Needs It?" presentation, and a demonstration of the Control System Self Assessment Tool (CS2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP provided control systems cyber security training, "Introduction to Control Systems for IT Professionals," at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP made presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP provided control systems cyber security training, "Solutions for Process Control Security," and a demonstration of the Control System Self Assessment Tool (CS2SAT), at the New Zealand Conference in Wellington, New Zealand.

- Upcoming events next week

  - On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:
    - Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
    - To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.
  - On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.
  - On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

  - The next monthly Control Systems Cyber Security Vendors Forum teleconference is on August 14th.

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

DRAFT/ PRE-DECISIONAL

Control Systems Security Program Weekly Summary Week of Dec 31 – Jan 4

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Dec 24 – Dec 28

- Dec 24-28, 2008 No significant outside events this week.
- Strategy for Control Systems Security. CSSP is developing the strategy to align federal and private programs and initiatives in response to GAO recommendation.
  - Initial work plan has been developed.
  - Next steps include briefings to PCIS, CSCSWG, and PCSF to achieve partner and stakeholder buy in
- Jan 14 – 17, 2008 SANS SCADA summit 2008, New Orleans, LA
  - The NCSD will sponsor Control System Cyber Security training
  - The following Process Control Systems Forum (PCSF) Working Group will meet:
    - ✓The Control Systems National Strategy Working Group
    - ✓Project Advisory WG
    - ✓Control Systems Cyber Security Vendor Forum WG
- Jan 14 – 17, 2008 The CSSP will:
  - ✓Release the Catalog of Control Systems Security- Recommendations for Standards Developers
  - ✓Release the NCSD online course “OPSEC for Control Systems “- Introduction to basic Operational Security principles in control system

Control Systems Security Program Weekly Summary Week of Dec 17 – Dec 21

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Dec 10 – Dec 14

- On December 11, the CSSP will host the monthly Control Systems Vendors Security Forum teleconference, topics of discussion will be:
  - National Strategy – Coordinating control system security.
  - Continue discussions to plan for January meeting at the SANS SCADA Summit to work on the Vendors Forum Charter

Control Systems Security Program Weekly Summary Week of Dec 03 – Dec 07

- On Tuesday, December 04, the CSSP will be providing an 8Hr Control System Cyber Security lecture at the United States Secret Service SCADA overview workshop at the Carnegie Mellon University in Pittsburg, PA.
- On Tuesday, December 04, the CSSP will be judging and attending the Cyber Security Awareness Week (CSAW) competitions at the Polytechnic University in Brooklyn, NY. This is a venue to discover the best interns.
- On Tuesday, December 04, the CSSP will participate in the Technical Vulnerability Discussion at the Idaho National Laboratory with SNL/PNNL/DOD OSD/DoE OE/ and DHS.
- On Wednesday, December 05, the CSSP will provide an eight minute presentation on the Control System cyber security self assessment tool (CS2SAT) at a webcast sponsored by Control Engineering magazine.
- On Wednesday, December 05, the CSSP will be presenting control systems common vulnerabilities/mitigations at the Marcus Evans Utility Cyber Security conference in Dallas, TX. The conference will take a look at the current challenges faced by utility companies in identifying and managing their operational critical cyber assets, talk about some of the regulatory compliance processes, and provide an opportunity to discuss the two big questions: “Where do we stand?” and “How much work will be needed to become compliant?”
- On Wednesday, December 05, the CSSP will participate in the unclassified Bi-weekly Chemical Sector teleconference. The purpose of the call is to provide a cyber situational awareness report which acts as a mechanism for disseminating US-CERT related vulnerability information and publications as well as any other cyber issues of concern to private members of the chemical sector. The teleconferences are open to all chemical facility owner/operators and plant managers.

Control Systems Security Program Weekly Summary Week of Nov 26 – Nov 30

- On Thursday, November 29, CSSP Deputy Director will participate in the Cross-Sector Cyber Security Work Group (CSCSWG) teleconference meeting. The group will be providing status updates of ongoing projects (like the Sector Specific Plan Review), special announcements, and informational briefings of broad interest to the group.

Control Systems Security Program Weekly Summary Week of Nov 19 – Nov 23

- On Tuesday, November 20, CSSP personnel along with engineers from Sandia National Laboratories, Idaho National Laboratory, and Department of Energy, will participate in a technical exchange meeting being held at the Idaho National Laboratory to discuss technical details of the Aurora vulnerability. Rescheduled for December 4th.

Control Systems Security Program Weekly Summary Week of Nov 12 – Nov 16

- On November 12, the Queensland University of Technology (QUT) and the University of South Australia will visit the Idaho National Laboratory (INL). INL will present the NCSD/CSSP program brief, tools, procurement language, recommended practices; and methods used as means for industry outreach. The QUT and University of South Australia will share their research on Critical Infrastructure (CI) with specific focus on incident response and forensic capabilities. Both universities have been involved in this research for several years, and have developed a great product that will assist in securing CI. The QUT has also requested a briefing on the NSTB program. Both Universities will be visiting other Department of Energy National Laboratories.
- On November 12, (b)(6) from the CSSP will participate in the Emerson Global Users Exchange Board of Directors Meeting in Austin, Texas.
- On November 13, The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - CS2SAT License w/ISA Announcement
    Updated Software – What are the changes from Beta version?
    ISA Pricing Structure
  - National Strategy – Coordinating control system security.
  - Continue discussion of last month, to plan for January meeting to work on the Vendors Forum Charter

Control Systems Security Program Weekly Summary Week of Nov 5 – Nov 9

- On 5 November, representatives from the CSSP will attend to monitor the Institute for Information Infrastructure Protection (I3P) Control System Security Awareness and Education Course: "Understanding Cyber Risks and Mitigation Strategies" in Houston, Texas.

Control Systems Security Program Weekly Summary Week of Oct 29 – Nov 2

- On 31 October, Deputy Director of CSSP will meet with representatives from the Water Sector at the Washington Marriott to discuss coordination and next steps in developing a water sector roadmap to control systems security
- On 29 October, Deputy Director of CSSP will meet with representatives of Baltimore Power and Light at their Baltimore, MD facility to discuss their implementation of the hardware mitigation to the control systems vulnerability.

Control Systems Security Program Weekly Summary Week of Oct 22 – Oct 26

- October 23 - 24 The CSSP will host a Lab Leadership Meeting in Washington D.C. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.

- October 24 – 26 at the Meridian 2007 Conference, Stockholm Sweden, the CS&C Chief of Staff will present "How Governments are Organized to Address Public-Private Sectors Interactions, Dealing with Process Control Security," and a representative from CSSP will be presenting "Process Control Systems Challenges, How Process Control Differs from IT." The Chief of Staff will also be participating in a panel discussion and discuss the importance of exercises for critical infrastructure protection.

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. (b)(6) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) ill deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Dec 31 – Jan 4

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Dec 24 – Dec 28

- Dec 24-28, 2008 No significant outside events this week.
- Strategy for Control Systems Security. CSSP is developing the strategy to align federal and private programs and initiatives in response to GAO recommendation.
  - Initial work plan has been developed.
  - Next steps include briefings to PCIS, CSCSWG, and PCSF to achieve partner and stakeholder buy in
- Jan 14 – 17, 2008 SANS SCADA summit 2008, New Orleans, LA
  - The NCSD will sponsor Control System Cyber Security training
  - The following Process Control Systems Forum (PCSF) Working Group will meet:
    - ✓The Control Systems National Strategy Working Group
    - ✓Project Advisory WG
    - ✓Control Systems Cyber Security Vendor Forum WG
- Jan 14 – 17, 2008 The CSSP will:
  - ✓Release the Catalog of Control Systems Security- Recommendations for Standards Developers
  - ✓Release the NCSD online course “OPSEC for Control Systems “- Introduction to basic Operational Security principles in control system

Control Systems Security Program Weekly Summary Week of Dec 17 – Dec 21

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Dec 10 – Dec 14

- On December 11, the CSSP will host the monthly Control Systems Vendors Security Forum teleconference, topics of discussion will be:
  - National Strategy – Coordinating control system security.
  - Continue discussions to plan for January meeting at the SANS SCADA Summit to work on the Vendors Forum Charter

Control Systems Security Program Weekly Summary Week of Dec 03 – Dec 07

- On Tuesday, December 04, the CSSP will be providing an 8Hr Control System Cyber Security lecture at the United States Secret Service SCADA overview workshop at the Carnegie Mellon University in Pittsburg, PA.
- On Tuesday, December 04, the CSSP will be judging and attending the Cyber Security Awareness Week (CSAW) competitions at the Polytechnic University in Brooklyn, NY. This is a venue to discover the best interns.
- On Tuesday, December 04, the CSSP will participate in the Technical Vulnerability Discussion at the Idaho National Laboratory with SNL/PNNL/DOD OSD/DoE OE/ and DHS.
- On Wednesday, December 05, the CSSP will provide an eight minute presentation on the Control System cyber security self assessment tool (CS2SAT) at a webcast sponsored by Control Engineering magazine.
- On Wednesday, December 05, the CSSP will be presenting control systems common vulnerabilities/mitigations at the Marcus Evans Utility Cyber Security conference in Dallas, TX. The conference will take a look at the current challenges faced by utility companies in identifying and managing their operational critical cyber assets, talk about some of the regulatory compliance processes, and provide an opportunity to discuss the two big questions: “Where do we stand?” and “How much work will be needed to become compliant?”
- On Wednesday, December 05, the CSSP will participate in the unclassified Bi-weekly Chemical Sector teleconference. The purpose of the call is to provide a cyber situational awareness report which acts as a mechanism for disseminating US-CERT related vulnerability information and publications as well as any other cyber issues of concern to private members of the chemical sector. The teleconferences are open to all chemical facility owner/operators and plant managers.

Control Systems Security Program Weekly Summary Week of Nov 26 – Nov 30

- On Thursday, November 29, CSSP Deputy Director will participate in the Cross-Sector Cyber Security Work Group (CSCSWG) teleconference meeting. The group will be providing status updates of ongoing projects (like the Sector Specific Plan Review), special announcements, and informational briefings of broad interest to the group.

Control Systems Security Program Weekly Summary Week of Nov 19 – Nov 23

- On Tuesday, November 20, CSSP personnel along with engineers from Sandia National Laboratories, Idaho National Laboratory, and Department of Energy, will participate in a technical exchange meeting being held at the Idaho National Laboratory to discuss technical details of the Aurora vulnerability. Rescheduled for December 4th.

Control Systems Security Program Weekly Summary Week of Nov 12 – Nov 16

- On November 12, the Queensland University of Technology (QUT) and the University of South Australia will visit the Idaho National Laboratory (INL). INL will present the NCSD/CSSP program brief, tools, procurement language, recommended practices; and methods used as means for industry outreach. The QUT and University of South Australia will share their research on Critical Infrastructure (CI) with specific focus on incident response and forensic capabilities. Both universities have been involved in this research for several years, and have developed a great product that will assist in securing CI. The QUT has also requested a briefing on the NSTB program. Both Universities will be visiting other Department of Energy National Laboratories.
- On November 12, Marty Edwards from the CSSP will participate in the Emerson Global Users Exchange Board of Directors Meeting in Austin, Texas.
- On November 13, The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - CS2SAT License w/ISA Announcement
    Updated Software – What are the changes from Beta version?
    ISA Pricing Structure
  - National Strategy – Coordinating control system security.
  - Continue discussion of last month, to plan for January meeting to work on the Vendors Forum Charter

Control Systems Security Program Weekly Summary Week of Nov 5 – Nov 9

- On 5 November, representatives from the CSSP will attend to monitor the Institute for Information Infrastructure Protection (I3P) Control System Security Awareness and Education Course: "Understanding Cyber Risks and Mitigation Strategies" in Houston, Texas.

Control Systems Security Program Weekly Summary Week of Oct 29 – Nov 2

- On 31 October, Deputy Director of CSSP will meet with representatives from the Water Sector at the Washington Marriott to discuss coordination and next steps in developing a water sector roadmap to control systems security
- On 29 October, Deputy Director of CSSP will meet with representatives of Baltimore Power and Light at their Baltimore, MD facility to discuss their implementation of the hardware mitigation to the control systems vulnerability.

Control Systems Security Program Weekly Summary Week of Oct 22 – Oct 26

- October 23 - 24 The CSSP will host a Lab Leadership Meeting in Washington D.C. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.

- October 24 – 26 at the Meridian 2007 Conference, Stockholm Sweden, the CS&C Chief of Staff will present "How Governments are Organized to Address Public-Private Sectors Interactions, Dealing with Process Control Security," and a representative from CSSP will be presenting "Process Control Systems Challenges, How Process Control Differs from IT." The Chief of Staff will also be participating in a panel discussion and discuss the importance of exercises for critical infrastructure protection.

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. Alan Paller (SANS) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) , an Australian government representative to collaborate on key steps to protect critical infrastructure.

Homeland Security

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

DRAFT/ PRE-DECISIONAL

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Homeland Security

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) , will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

DRAFT/ PRE-DECISIONAL

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing.

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. Perry Pederson will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the UTC-NER Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Homeland Security

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) , briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. Alan Paller (SANS) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director Vishant Shah will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. Alan Paller (SANS) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Oct 29 – Nov 2

- On 31 October, Deputy Director of CSSP will meet with representatives from the Water Sector at the Washington Marriott to discuss coordination and next steps in developing a water sector roadmap to control systems security
- On 29 October, Deputy Director of CSSP will meet with representatives of Baltimore Power and Light at their Baltimore, MD facility to discuss their implementation of the hardware mitigation to the control systems vulnerability.

Control Systems Security Program Weekly Summary Week of Oct 22 – Oct 26

- October 23 - 24 The CSSP will host a Lab Leadership Meeting in Washington D.C. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.

- October 24 – 26 at the Meridian 2007 Conference, Stockholm Sweden, the CS&C Chief of Staff will present "How Governments are Organized to Address Public-Private Sectors Interactions, Dealing with Process Control Security," and a representative from CSSP will be presenting "Process Control Systems Challenges, How Process Control Differs from IT." The Chief of Staff will also be participating in a panel discussion and discuss the importance of exercises for critical infrastructure protection.

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. (b)(6) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) , briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Homeland Security

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Nov 5 – Nov 9

- On 5 November, representatives from the CSSP will attend to monitor the Institute for Information Infrastructure Protection (I3P) Control System Security Awareness and Education Course: "Understanding Cyber Risks and Mitigation Strategies" in Houston, Texas.

Control Systems Security Program Weekly Summary Week of Oct 29 – Nov 2

- On 31 October, Deputy Director of CSSP will meet with representatives from the Water Sector at the Washington Marriott to discuss coordination and next steps in developing a water sector roadmap to control systems security
- On 29 October, Deputy Director of CSSP will meet with representatives of Baltimore Power and Light at their Baltimore, MD facility to discuss their implementation of the hardware mitigation to the control systems vulnerability.

Control Systems Security Program Weekly Summary Week of Oct 22 – Oct 26

- October 23 - 24 The CSSP will host a Lab Leadership Meeting in Washington D.C. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.

- October 24 – 26 at the Meridian 2007 Conference, Stockholm Sweden, the CS&C Chief of Staff will present "How Governments are Organized to Address Public-Private Sectors Interactions, Dealing with Process Control Security," and a representative from CSSP will be presenting "Process Control Systems Challenges, How Process Control Differs from IT." The Chief of Staff will also be participating in a panel discussion and discuss the importance of exercises for critical infrastructure protection.

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. (b)(6) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

Control Systems Security Program Weekly Summary Week of January 16 – January 19

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team meeting on January 18, 2007, to address a newly discovered control systems vulnerability.
- The CSSP is meeting with the Chief CIO, US Army Corp of Engineers at DOD headquarters on January, 19, 2007 to discuss possible inclusion of DOD security requirements in the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). This meeting is a result of a previous pilot effort of the CS2SAT with the Corps of Engineers.
- The CSSP will host a Control Systems Standards Support Strategy meeting on Jan 18. The meeting will help coordinate control systems standards activities between NCSD, NIST, and the national laboratories.
- The CSSP will participate in the Control Systems Malware Identification task team meeting at Lawrence Livermore National Laboratory the week of January 16. This group is working to determine the characteristics of control systems malware to develop detection signatures and recovery strategies.
- The CSSP is participating in the InfraGard Nations Capital Members Alliance (INCMA) General Membership meeting in Vienna, VA on January 17, 2007.

Control Systems Security Program Weekly Summary Week of January 8 – January 12

- The Control Systems Security Center will provide multiple training sessions on control systems security for the energy working group of the Pacific NorthWest Economic Region (PNWER). PNWER is a statutory, public/private partnership composed of legislators, governments, and businesses in the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on January 9, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. A major point of discussion will be potential issues surrounding the new times for shifting to Day Light Savings Time (DLST).

National Cyber Security Division

SI Branch – Control Systems

Weekly Summary for 2007

Homeland Security

~~DRAFT/ PRE-DECISIONAL~~

Control Systems Security Program Weekly Summary Week of Nov 19 – Nov 23

- On Tuesday, November 20, CSSP personnel along with engineers from Sandia National Laboratories, Idaho National Laboratory, and Department of Energy, will participate in a technical exchange meeting being held at the Idaho National Laboratory to discuss technical details of the Aurora vulnerability.

Control Systems Security Program Weekly Summary Week of Nov 12 – Nov 16

- On November 12, the Queensland University of Technology (QUT) and the University of South Australia will visit the Idaho National Laboratory (INL). INL will present the NCSD/CSSP program brief, tools, procurement language, recommended practices; and methods used as means for industry outreach. The QUT and University of South Australia will share their research on Critical Infrastructure (CI) with specific focus on incident response and forensic capabilities. Both universities have been involved in this research for several years, and have developed a great product that will assist in securing CI. The QUT has also requested a briefing on the NSTB program. Both Universities will be visiting other Department of Energy National Laboratories.
- On November 12, (b)(6) from the CSSP will participate in the Emerson Global Users Exchange Board of Directors Meeting in Austin, Texas.
- On November 13, The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - CS2SAT License w/ISA Announcement
    Updated Software – What are the changes from Beta version?
    ISA Pricing Structure
  - National Strategy – Coordinating control system security.
  - Continue discussion of last month, to plan for January meeting to work on the Vendors Forum Charter

Control Systems Security Program Weekly Summary Week of Nov 5 – Nov 9

- On 5 November, representatives from the CSSP will attend to monitor the Institute for Information Infrastructure Protection (I3P) Control System Security Awareness and Education Course: "Understanding Cyber Risks and Mitigation Strategies" in Houston, Texas.

Control Systems Security Program Weekly Summary Week of Oct 29 – Nov 2

- On 31 October, Deputy Director of CSSP will meet with representatives from the Water Sector at the Washington Marriott to discuss coordination and next steps in developing a water sector roadmap to control systems security
- On 29 October, Deputy Director of CSSP will meet with representatives of Baltimore Power and Light at their Baltimore, MD facility to discuss their implementation of the hardware mitigation to the control systems vulnerability.

Control Systems Security Program Weekly Summary Week of Oct 22 – Oct 26

- October 23 - 24 The CSSP will host a Lab Leadership Meeting in Washington D.C. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.

- October 24 – 26 at the Meridian 2007 Conference, Stockholm Sweden, the CS&C Chief of Staff will present "How Governments are Organized to Address Public-Private Sectors Interactions, Dealing with Process Control Security," and a representative from CSSP will be presenting "Process Control Systems Challenges, How Process Control Differs from IT." The Chief of Staff will also be participating in a panel discussion and discuss the importance of exercises for critical infrastructure protection.

Control Systems Security Program Weekly Summary Week of Oct 15 – Oct 19

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of Oct 8 – Oct 12

- October 9 – The CSSP will host the monthly teleconference Vendors Forum, topics of discussion will be:
  - Vendor Forum's charter (DRAFT).
  - The CSSP Deputy Director will brief on NCSD's responsible vulnerability disclosure process.
- October 10 – The CCSP will discuss the Catalog of Control Systems Security Recommendations for Standards developers at the American Public Transportation Association (APTA) Annual Meeting in Charlotte, NC
- October 11-12 - National Cyber Security Division will host Control Systems Cyber Security training at Glebe Rd facility, 97 attendees from federal agencies and departments supporting control systems security have registered.
  - October 11 – Solutions for Process Control Security (2 sessions)
  - October 12 - Introduction to Control Systems for IT Professionals

Control Systems Security Program Weekly Summary Week of Oct 1 – Oct 5

- Tuesday, October 02 through 04, 2007 CSSP staff will participate in several sessions at the Instrumentation, Systems, and Automation Society (ISA) Expo 2007 in Houston, TX (Houston Reliant Center). CSSP will have an exhibit booth, present a Control Systems Cyber Security Self Assessment Tool (CS^2SAT) paper and a Defense In Depth paper, and lead a Standards Harmonization Panel discussion.
- Wednesday, October 4, 2007 CSSP staff will give a presentation on Control systems Security Initiatives at the 2007 Critical Infrastructure Protection Congress in San Diego, CA. The Critical Infrastructure Protection Committee (CIPC) is sponsored by the Information Sharing and Analysis Centers Council (ISAC Council) and InfraGard.

Control Systems Security Program Weekly Summary Week of Sept 24 – Sept 28

- On September 26 – 28, 2007 CSSP staff will participate in the review meeting for the I3P Consortium, and the process control project team, being held at the US Military Academy in West Point, NY. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On September 24, 2007 : CSSP staff will participate in New York Government Workshop to "C" level executives of New York State and local municipalities in Albany, NY. CSSP staff will give a presentation on common vulnerabilities, show the chemical sector cyber security video, and announce 2 webcast dates for CS2SAT demonstrations in October. Alan Paller (SANS) is also scheduled to give Cyber Security awareness presentation.
- On Monday, September 24, 2007, CSSP Deputy Director (b)(6) will present the CSSP overview brief at the Electric Power Research Institute (EPRI) / Energy Information Security Advisors (EIS) Power Delivery & Markets Area Council Meeting in Chantilly, VA. CSSP staff will also provide a briefing on the CSSP developed CS2SAT tool

Control Systems Security Program Weekly Summary Week of Sept 15 – Sept 21

- On September 18 The CSSP will give a program briefing of the Control Systems Security Program at the 3rd Annual E-Sec NW [Energy Security Northwest] CIPS Summit on compliance to the NERC Critical Infrastructure Protection Standards, CIP-002 through CIP-009 (CIPS), in Portland, OR.
- On September 20 The CSSP will give a perspective on Cyber Security in the Water Sector at the Cyber Security in the Water Sector: Securing Control Systems conference in San Jose, CA. The CSSP supports the American Water Works Association's effort in developing a strategic plan/roadmap for addressing water sectors needs in cyber security.

Control Systems Security Program Weekly Summary Week of Sept 08 – Sept 14

On September 10-14 The CSSP will participate in the user group meeting through staffing an exhibit booth at the Emerson Global Users Exchange in Grapevine, Texas. Note: (b)(6) CSSP Outreach, is Chairman of the Emerson Exchange for 2007.

Control Systems Security Program Weekly Summary Week of Sept 01 – Sept 07

- On September 6, the CSSP will give a presentation on the Control Systems Cyber Security Self Assessment Tool (CS^2SAT) and its use to understand how well an asset owner is meeting the CIP standard's requirements, at the United Telecom Council- North American Electric Reliability Corporation (UTC-NERC) Cyber Security Workshop in Washington, DC.

Control Systems Security Program Weekly Summary Week of Aug 27 – August 31

- On August 28-30 the CSSP will give a presentation on the U5 workshop at the annual REDTEAM meeting in Washington, DC. The conference will address two broad application areas: (a) red teaming and adversary-based assessments and (b) adversary modeling.
- On August 28 the CSSP will give a PCSF up date to the Cross Sector Working Group in Washington DC

Control Systems Security Program Weekly Summary Week of Aug 20 – August 24

- On August 21st the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. The topic for August will be on Vendor Assessments. There will be three guest speakers, one each from INL, Wurldtech, and ISA. Each speaker will provide information about their assessment program or proposed guidance. The purpose of this topic is to demonstrate what others in industry are doing and that the CSSP through INL are providing assessments that the industry is not doing

Control Systems Security Program Weekly Summary Week of Aug 11 – August 17

- On Aug 13th the CSSP Director will participate in a Control Systems vulnerabilities panel discussion at the 2007 Applied Control Systems in Knoxville, Tennessee.
- On Aug 14th the CSSP will present an overview of the DHS CSSP, the CSSC work on Security Metrics, and LDRD Attack Graph efforts at the MIT Lincoln Labs in Lexington, MA.
- On Aug 16th the CSSP will conduct a meeting with the Instrumentation, Systems, and Automation Society (ISA) with regards to potential licensing and distribution of the Control Systems Cyber Security Self Assessment Tool (CS2SAT) on August 16th in Knoxville, TN
- On Aug 16th the CSSP will participate in the Bulk Power Transmission System: How It Works and How To Make It More Reliable Seminar in Washington DC to gain a better understanding of the physical and operational characteristics of the electrical grid to support the development of plausible cyber attack scenarios on the control system scenarios.

Control Systems Security Program Weekly Summary Week of Aug 4 – August 10

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 28 – August 3

- No significant outside events this week.

Control Systems Security Program Weekly Summary Week of July 23 – July 27

On July 23rd and July 24th CSSP will host a two-day information and coordination meeting on the PCSF, and training and technology transfer for the control systems cyber security. The participants will include: PCSF, DOE, I3P, LOGIIC,PNNL, Sandia Laboratory, and TSWG representatives. The purpose of the meeting is to:

- Develop new short- and long-term strategies for the Process Control Systems Forum (PCSF), and to solicit ideas for the PCSF's growth and vision from key participants and stakeholders
- To develop an understanding of the control systems cyber security tools and training offered by federal organizations, and potentially to begin to develop a coordinated vision on how we offer these products to our constituencies and how to transfer them to other non-government organizations.

On July 23rd the CSSP will participate in a roundtable discussion and exhibit a DHS/CSSP booth at the Waterpower XV Conference in Chattanooga TN. The discussion will entail current security standards for critical and non-critical facilities and how are those standards implemented and enforced.

On July 23rd the CSSP Director will participate in a conference call with Shell International Exploration and Production B.V. to discuss the use of CSSP Control Systems courses as their general awareness on cyber security in the process control domain training standard.

Control Systems Security Program Weekly Summary Week of July 16 – July 22

On July 19th the CSSP Director, (b)(6) will meet with (b)(6) an Australian government representative to collaborate on key steps to protect critical infrastructure.

Control Systems Security Program Weekly Summary Week of July 09 – July 15

On July 12th CSSP will lead a Kick-Off meeting for SCADA Cyber Attack Alert Tool (TSWG SCADA W91CRB-07-C-0070) in Washington D.C. The purpose of the project is to develop a SCADA Cyber Attack Alert Tool system to alert operators to the existence, nature, and extent of cyber attacks and report that information based on a standard set of attack definitions against geospatially distributed, resource limited, and time-critical systems.

Control Systems Security Program Weekly Summary Week of July 02 – July 08

On July 2nd the CSSP Director, (b)(6) will participate in the JASON (July-August-September-October-November) Power Grid Study in San Diego, California. JASON is an independent group of scientists that advises the U.S. government on matters of science and technology. Its sponsors include the Department of Defense (frequently DARPA and the U.S. Navy), the Department of Energy, and the U.S. intelligence community. Most of the resulting Jason reports are classified.

Control Systems Security Program Weekly Summary Week of June 25 – June 29

- On June 25th the CSSP will provide control systems cyber security training, “Control Systems Cyber Security - Who Needs It?” presentation, and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the American Water Works Association conference- AWWA-ACE 2007 in Toronto, ON, Canada.
- On June 25th the CSSP will provide control systems cyber security training, “Introduction to Control Systems for IT Professionals,” at the GFIRST National Conference in Orlando, FL. US-CERT Operations staff and Federal Partners received this training on May 21st & 22nd.
- On June 25th the CSSP will make presentations on the NIST publication 800-53, the Catalog of Security Requirements (draft), and the Cyber Security Procurement Language for Control Systems (draft) document to the SP99 Working Group 4 meeting in Scottsdale, AZ.
- On June 25th – 27th the CSSP will provide control systems cyber security training, “Solutions for Process Control Security,” and a demonstration of the Control System Self Assessment Tool (CS^2SAT), at the New Zealand Conference in Wellington, New Zealand.
- The CSSP Director, (b)(6) briefed on Control System Vulnerability (Aurora) to :
  - June 25th - the Dam Sector.
  - June 25th - the Australian Critical Infrastructure representatives at the Australian Embassy.
  - June 26th - the EMP (Electro Magnetic Pulse) Presidential Commission.
  - June 28th - the GAO on Aurora project and its mitigation strategy.
  - June 28th - the Senate’s HSGAC (Homeland Security and Government Affairs Committee) on Aurora project and its mitigation strategy.

Control Systems Security Program Weekly Summary Week of June 18 – June 22

- On June 19h the CSSP will provide control systems cyber security training, Introduction to Control Systems for IT Professionals, at the Air Force Training conference in Ft. Walton Beach, FL.

Control Systems Security Program Weekly Summary Week of June 11 – June 15

- On June 12th the CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- On June 13, CSSP staff will give a 30-45 min. presentation on control systems cyber security to the Utility Executive Course at University of Idaho. For over 50 years, the Utility Executive Course has been preparing industry leaders with the knowledge and skills they need to produce business results. UEC has earned a worldwide reputation as the premier industry-driven executive education program designed specifically for utility leaders.
- On June 12th the CSSP will provide training 4 different control systems cyber security training sessions at the Siemens User Group conference in Orlando, FL.
- On June 12th, CSSP staff will attend the 2007 : FERC DAM Security Conference in Denver, CO. The FERC is hosting a 2 day workshop on dam security open (and free) to all private and federal dam owners/operators.

Control Systems Security Program Weekly Summary Week of June 4 – June 8

- On June 5 – 6, 2007 CSSP staff will participate in the review meeting for the I3P Consortium being held at Carnegie Mellon University, Pittsburgh. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- On June 6, 2007 CSSP will hold the next facilitated Federal Partners coordination meeting to outline the scope and content of the Federal Coordinating Strategy for Securing Control Systems. This stakeholder-driven plan will outline how the federal government will coordinate and share information on control systems activities and can serve as a central framework for coordinating federal activities. The intent of the plan is to define a common set of high-level goals, outline the key requirements of effective federal programs, and identify effective coordination mechanisms. While this plan is intended to reflect the needs of the entire control systems community, it is primarily intended as a strategy to improve federal coordination.

Control Systems Security Program Weekly Summary Week of May 29 – June 1

- On May 29, 2007 CSSP staff will participate in the Washington, DC InfraGard meeting. The CSSP team will discuss ways to share information and collaborate with the new SCADAGard working group.

Control Systems Security Program Weekly Summary Week of May 21 – May 25

On May 21st & 22nd the CSSP will be providing an 8-hour training course titled "Control Systems Security for IT Professionals" to US-CERT Operations staff. And, on May 23rd, the CSSP will be providing a 4-hour training course on Control Systems Security for the Control Systems Federal Partners Group.

On May 21st, CSSP staff will attend the S&T Meeting in Washington, DC to participate in discussions of National Laboratory Capabilities.

On May 24th, CSSC representatives will support the 2007 WERF Webcast. The title of the web cast is "Cyber Security Tool: Protecting Water and Wastewater Process Control Systems from Online Attacks."

On May 20th through May 24rd CSSC representatives will be attending the ABB 2007 Spring User's Group Meeting in Scottsdale, AZ in support of the CSSP outreach mission.

Control Systems Security Program Weekly Summary Week of May 14 – May 18

- On May 15 and16, the quarterly CSSP Lab Leadership Meeting will be held at Lawrence Livermore National Laboratory (LLNL), in Livermore, California. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- On May 15 and 16, CSSP staff will participate in a panel discussion on standards harmonization at the Platts 5th Annual Cybersecurity for Utilities Conference, Houston, Texas. The conference is attended by cyber security, information security, information technology, energy systems analyst, critical infrastructure protection, energy management systems, and corporate security professionals.

Control Systems Security Program Weekly Summary Week of May 7 – May 12

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on May 8th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- CSSP staff will provide a CSSP program brief to the Utilities Telecom Council's Annual Conference and Exposition—UTC Telecomm 2007, in Austin TX on May 6-9 . The conference is geared towards telecommunications, information technology and networking professional at utilities.
- CSSP staff will attend the Cyber Security Program Spring General Meeting of Chem ITC in Miami, FL, from May 09 – 11, 2007. The meeting's emphasis is on challenges that are relevant to industry and provides an excellent opportunity for the industry's cyber security professionals to share experiences and learn what industry peers are doing to face cyber security challenges head on.

Control Systems Security Program Weekly Summary Week of April 30 – May 4

- The CSSP will host a week long control systems cyber security training conference, April 30 through May 4. The conference will bring together control systems security experts from the U5 Countries (US, UK, Canada, Australia, and New Zealand) for informational and coordinating briefings, training sessions, and a control systems Red Team exercise. (b)(6) will deliver the keynote address for CS&C.

Control Systems Security Program Weekly Summary Week of April 23 – April 27

- The CSSP will provide a control systems cyber security overview briefing at the ISSA Boise Chapter 4th Annual InfoSec Conference, Boise, ID, on April 25. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Control Systems Security Program Weekly Summary Week of April 14 – April 20

- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on April 17th, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security.
- The CSSP will be participating in the American Chemistry Council's (ACC's) Security Conference and Exposition – ChemSecure in Washington, D.C. April 17-19. ChemSecure is designed to support ACC member's efforts to implement the DHS regulatory framework requirements into their existing systems developed for the Responsible Care Security Code.
- The CSSP will provide the CSSP Program Brief at the PAS Process Matters 2007 Conference in Galveston, TX on April 18. The conference theme – Innovate! Collaborate! Simplify! echoes the current needs and expectations of the industry. Major global companies such as ExxonMobil, Shell, BP, DuPont, DOW, ARAMCO, Chevron and many others are expected to attend.

Control Systems Security Program Weekly Summary Week of April 9 – April 13

- CSSP staff will attend the Defense Industrial Base Critical Infrastructure Protection Conference April 10 – 12 in Miami, FL. The conference is designed to enhance public and private sector collaboration and mutual understanding of the critical roles of the federal, state and municipal governments, and defense industry owners and operators in building a resilient defense industrial base.

Control Systems Security Program Weekly Summary Week of April 2 – April 6

- No significant outside activities this week.

Control Systems Security Program Weekly Summary Week of March 26 – March 30

- On Monday, March 26, 2007 CSSP staff will attend the Risk Symposium 2007 – Risk Analysis for Homeland Security and Defense Theory and Application in Santa Fe, New Mexico. The goal of the meeting is to support sector work and RAMCAP.
- On March 27, 2007 CSSP staff will participate in the Industrial Control Systems (ICS) Workshop at NIST in Gaithersburg, Maryland. The agenda will include work on NIST SP-800-53 and SP-800-53A, NERC CIP Analysis, outreach plans to Inspectors General relating to FISMA requirements, and NIST SP-800-82

Control Systems Security Program Weekly Summary Week of March 19 – March 23

- On Monday, March 19, 2007 CSSP staff will attend the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection in Hanover, New Hampshire (Dartmouth College). The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policymakers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in critical infrastructure protection.
- On March 21, 2007 CSSP staff will participate in the review meeting for the I3P Consortium Meeting Institute for Security Technology Studies (ISTS) in Hanover, NH (Dartmouth College).
- During the week of March 19 through 23, CSSP staff will accompany the Nuclear Regulator Commission as an observer on a site audit at Calvert Cliffs Nuclear Power Plant in Lusby, Md.

Control Systems Security Program Weekly Summary Week of March 12 – March 16

- The CSSP will participate in an Emerson Process Management users workshop in Vancouver, BC, Canada on March 15, 2007.
- The CSSP large scale validation test of a significant control systems vulnerability (Pandora) was successfully completed at the Idaho National Laboratory on March 4, 2007. Results and findings from the test are being documented and significant follow-on activities are anticipated. The Tiger Team formed to coordinate activities for this vulnerability will meet on March 13. to U/S Foresman is scheduled to be briefed the afternoon of March 13. Briefings to Secretary Chertoff, House Homeland Security Committee, and White House Homeland Security Council are anticipated.

Control Systems Security Program Weekly Summary Week of March 5 – March 9

- The CSSP will host a face to face Control Systems Cyber Security Vendors Forum meeting on March 5 in Atlanta, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. This is the first “live” meeting of the vendors who have participated in the monthly teleconference sponsored by CSSP.
- The Process Control Systems Forum (PCSF) will host its annual conference March 6 through 8 in Atlanta, GA. Deputy A/S Landis is the keynote speaker. The PCSF is the primary outreach arm of the CSSP. The event is expected to attract over 300 attendees, and will feature sessions covering solutions to control system security issues, security training sessions, and other meetings of the PCSF working group.

Control Systems Security Program Weekly Summary Week of February 25 – March 2

- The CSSP is conducting the scheduled large scale validation test of a significant control systems vulnerability (Pandora) at the Idaho National Laboratory on February 25. Representatives from DHS, DOD, DOE, the UK, Canada, and other federal and industry partners will be on hand to observe the test.

Control Systems Security Program Weekly Summary Week of February 19 – February 23

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). CSSP is installing target test equipment in preparation for large scale test of vulnerability.
- CSSP is participating in Emerson Global Users Exchange in Austin, Texas on February 19, 2007.
- CSSP is participating in a meeting between DHS and NIST in Washington, DC on February 22, 2007, to discuss control systems standards efforts and activities.

Control Systems Security Program Weekly Summary Week of February 12 – February 16

- CSSP will hold a Lab Leadership meeting, Houston, Texas on February 13 and 14. The leadership meeting brings together representatives from DHS and the national laboratories that perform the technical work of the Control Systems Security Center of the CSSP – Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Lawrence Livermore National Laboratory. The leadership discuss emerging technologies, vulnerabilities, research goals, and implementation plans for reducing cyber risk for control systems.
- CSSP will attend the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop in Houston, Texas on February 15 and 16. The I3P is a DHS-funded consortium that includes academic institutions, federally-funded labs and non-profit organizations to bring experts together to identify and help mitigate threats aimed at the U.S. information infrastructure.
- The CSSP will host the monthly Control Systems Cyber Security Vendors Forum teleconference on February 13, with emphasis on facilitating collaboration between government and vendors and providing an open forum to discuss common issues that affect control systems security. Agenda items include potential issues surrounding the new times for shifting to Daylight Savings Time (DST), and refining the agenda for the face to face vendor forum meeting to be held in Atlanta on March 5th.

Control Systems Security Program Weekly Summary Week of February 5 – February 9

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a significant control systems vulnerability (Pandora). Coordinating inputs for briefing on Pandora to U/S Foresman.
- Participating in a Canadian SCADA Collaboration meeting in Ottawa, Ontario on February 5-6, 2007. The CSSP will provide Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP) a CSSP program overview and control systems cyber security training.
- CSSP is working with US-CERT on developing an information bulletin that will provide guidance to critical infrastructure owners and operators on the new Daylight Savings Time changeover schedule specified in the Energy Policy Act of 2005 (second Sunday in March and first Sunday in November). Plans are to post information bulletin on Control Systems Security Program Website.

Control Systems Security Program Weekly Summary Week of January 29 – February 2

- The CSSP is continuing interagency and internal DHS coordination of an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address significant control systems vulnerability (Pandora). Planning for second Interagency Pandora Tiger Team meeting for week of January 29th.
- Participating in a meeting attended by DHS, Idaho National Laboratory (INL) and the Institute for Information Infrastructure Protection(I3P) to discuss control systems security efforts on February, 1, 2007.

Control Systems Security Program Weekly Summary Week of January 22 – January 26

- The CSSP is coordinating an Office of Cyber Security and Telecommunications (CS&T) and Office of Infrastructure Protection (IP) co-lead Tiger Team effort to address a newly discovered control systems vulnerability. The current plan is to brief the Under Secretary for Preparedness on Tiger Team progress on January 26, 2006.
- CSSP Director will provide briefing to UK National Infrastructure Security Co-ordination Centre (NISCC) on control systems vulnerability (Pandora).
- The CSSP will participate in the S4 SCADA Security Symposium in Miami, Florida on January 24 – 25, 2007. The S4 is a 2-day symposium with multiple technical presentations on SCADA security research.
- The CSSP will participate in the Microsoft Manufacturing Users Group (MSMUG) meeting in Seattle, Washington on January 24-26, 2007.

(b)(6)

From: (b)(6)
Sent: Tuesday, October 09, 2007 3:30 PM
To:
Cc: (b)(6)
Subject: (FOUO) RE: Lessons Learned - Inputs
Attachments: DHS Auroroa SOP Master-w-Appendices A&B-rev draft 2.doc

Follow Up Flag: Follow up
Flag Status: Flagged

(b)(6)

(b)(5)

(U) Thanks and look forward to working with you on the above.

- (b)(6) , OIP/POD/Cross Sector Specialist

From: (b)(6)
Sent: Tuesday, October 09, 2007 2:23 PM
To:
Cc: ' (b)(6)
Subject: RE: Lessons Learned POC?

Hi (b)(6)
I can be reached at
Office
cell: 7 (b)(6)
I look forward to hear from you.
Thank you,
(b)(6)

From: (b)(6)
Sent: Tuesday, October 09, 2007 12:55 PM
To:
Cc: (b)(6)
Subject: RE: Lessons Learned POC?

(b)(6) please follow up with (b)(6)

From: (b)(6)
Sent: Tuesday, October 09, 2007 8:08 AM
To:
Cc: (b)(6)
Subject: Lessons Learned POC?

(b)(6)

I lost the phone number and name for your Lessons Learned POC. Please re-send. Thanks.

(b)(6)

DHS/OIP/Cross Sector Specialist
NAC:
SSA EMO: (b)(6)

(b)(6)

From: (b)(6)
Sent: Thursday, February 21, 2008 10:47 AM
To: Vendor Forum; DHS - participants for Vendor Call; (b)(6)
Subject: Vendor Forum Minutes
Attachments: 20080212 Minutes-Vendor Forum Call.doc; 4-General Mitigations Measures.ppt; 2-General CSV Brief TER.ppt

Attached are the vendor forum conference call minutes. Please reply with any corrections you feel should be made.

It was suggested that this group develop 5 bullets of lessons learned of what when bad with the Aurora mitigation disclosure process and what needs to be improved. These lessons learned will be provided to (b)(6) (b)(6) nd others at DHS. It is recommended that all Vendor Forum Members submit their concerns and suggestions for improvement to (b)(6) by March 7, 2008.

NOTE: also attached are the presentations that were discussed during the conference call. The presentations are labeled **For Official Use Only**, which means that they are not to be distributed or shared with others. The information is sensitive and is provided on a need to know basis.

Mark your calendars for the next Vendor Forum conference call on March 11, 2008, at 3:30 PM Eastern time.

Have a great day!

NOTE This message was unable to be scanned for viruses because it is encrypted. If you are unsure of the source of this message, please discard.

(b)(6)

From: Garcia, Greg
Sent: Friday, June 29, 2007 6:13 PM
To: CS&C Office
Cc: Jamison, Robert; Hanna-Ruiz, Jeanette
Subject: CS&C Report
Attachments: CSC Priorities.ppt; CS&C Strategic Plan.doc

Follow Up Flag: Follow up
Flag Status: Flagged

To All Staff,

Before some of us embark on July 4 week festivities, I wanted to take a moment to give you all an update on recent activities in CS&C.

As many of you know, CS&C senior staff met offsite June 14-15 in Solomon's Maryland to engage in team building discussions and review progress on our strategic plan. I have attached for your information our Strategic Plan and an overview of our highest priorities.

The offsite gave senior managers an opportunity to assess the current state of the Office of Cyber Security and Communications and how we can improve the quality of the workplace and our work.

During the two day offsite, we all shared perspectives on the challenges that each of us faces as managers, and that we face as an organization, noting in particular the pace and quantity of demands placed on the organization from numerous external and internal stakeholders. There was an acknowledgment that the best way for us to manage in our high intensity, dynamic environment that has been through several leadership changes is to ensure that we are clear on our own priorities, execute on them in an efficient, measurable way, and clearly articulate our mission and accomplishments. Doing so conveys to stakeholders who have influence over our activities that we are purposeful, disciplined and effective.

Please know that as this organization matures, division heads (b)(6) and (b)(6) will be working with you and your managers to continually strengthen our capabilities, leverage our resources, streamline our processes and recognize and reward the hard work you do every day.

At the offsite we also invited key partners from within DHS, including senior representatives from the Office of Policy, the Private Sector Office and the Office of Legislative Affairs, to summarize their responsibilities as they involve CS&C and how we can continue to work together to leverage each other's expertise and positions within the larger organization.

The Office of Policy, for example, continues to be a strong partner and resource for ensuring that CS&C's equities are represented and coordinated within DHS, as they strive to convey "One DHS" to our external stakeholders. The Private Sector Office, similarly, assists CS&C by ensuring that our outreach and partnership with the private sector is coordinated across the DHS components that may have overlapping interests in enlisting private sector engagement.

We also discussed recommendations offered by many of you, through our "Recommendations Box", which will continue to be available to receive any additional recommendations you may have. I want

to thank all of you for taking the time to think about and forward ideas for how CS&C as an organization can improve our processes, planning, and office culture. This is the kind of participation and leadership from each and every one of you that we want to encourage and act upon. While many of the recommendations address policy suggestions that need to be considered at the DHS, or government-wide level, others are indeed what we in CS&C management have been working to improve upon as discussed above. However, one excellent suggestion, which I will make effective immediately, is that within CS&C I am instituting a business casual dress policy for the summer. This applies anytime during the week except when you have meetings with stakeholders outside DHS where the expectation and our credibility are based on more formal business attire.

Also, within the next couple of weeks, CS&C will be rolling out our first Employee Handbook, which will provide new and current employees with guidelines for office processes and conduct, HR policies, etc. I am confident you will find this useful and unifying for all new hires and for all current employees and management.

Finally, so that I and senior management can stay in touch with you on a regular basis and better facilitate our collective resolve around our shared mission, I am beginning a new "Brown Bag Lunch Series" on the (tentatively) second Friday of every month in the 11th floor conference room, beginning July 13. The themes will differ from month to month, ranging from open discussion with the Assistant Secretary, program briefs from senior and program staff, and guest speakers from outside CS&C. This will be a good opportunity for folks from across CS&C to relax around the lunch table, get to know each other and our responsibilities better, and exchange ideas about addressing the Secretary's goal of organizational excellence.

I want to wish all of you a very festive Fourth of July holiday, and to remind you how important and valued the contributions are that each one of you makes to protect our homeland. It is because of you that Americans across the country can enjoy and celebrate the freedoms that this holiday symbolizes.

Happy Independence Day, and please use good judgment on the road and with others, be safe, be alert and be patriotic!

Greg

Greg Garcia
Assistant Secretary
Cyber Security and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Arlington, VA 22201
(
((b)(6)

(b)(6)

From: (b)(6)
Sent: Friday, August 31, 2007 12:40 PM
To: (b)(6)
Cc: (b)(6) (b)(6)
Subject: RE: Program plan template
Attachments: CSSP Program Plan 20070711 v00_no budget.doc

Hi (b)(6)

I am a little confused by your question because we revised and updated the program plans using the new template at the end of May. All the program plans were approved by NCSD leadership prior to the CS&C offsite. I have attached the approved version in the appropriate template, but without budget data. Please let me know if I can be of further assistance.

Thanks,
(b)(6)

(b)(6)
Booz Allen Hamilton
Client: National Cyber Security Division
Department of Homeland Security
Office:
Mobile:
E-mail: (b)(6)

From: (b)(6)
Sent: Friday, August 31, 2007 12:26 PM
To: (b)(6)
Subject: Program plan template

Hi (b)(6)
Do you have or know where we can get a copy of the Program Plan template? Also, what is the approval chain for the Program Plan?
Thank you,
(b)(6)

****

(b)(6)
Securicon, LLC
Client: Department of Homeland Security
National Cyber Security Division
Control Systems Security Program
****
Office:
Mobile:
DHS E-m (b)(6)
Securico

****

From: (b)(6)
Sent: Tuesday, March 20, 2007 1:54 PM
To:
Cc: (b)(6)
Subject: FW: Tiger Team Status Brief (2)

Attachments: aurora test initial video E.zip

(b)(6)

As you requested, here is email 2 of 3.

Regards,

(b)(6)

Securicon LLC

Client: NCSD CSSP

Department of Homeland Security

(b)(6)

From: (b)(6)
Sent: Thursday, March 15, 2007 12:00 PM

(b)(6)

Subject: Tiger Team Status Brief (2)

(b)(6)

Pages 8 through 14 redacted for the following reasons: Duplicate

Diedrich, John

From: (b)(6)
Sent: Thursday, January 28, 2010 9:43 AM
To:
Subject: CSET - (b)(6) N2010

Follow Up Flag: Follow up
Flag Status: Flagged

Thank you for your inquiry concerning the Cyber Security Evaluation Tool (CSET). The DHS National Cyber Security Division is reviewing your request.

Unless otherwise notified, you will receive a DVD copy of CSET via FedEx within a few days.

CSET Program Office
National Cyber Security Division
U.S. Department of Homeland Security
CSET@dhs.gov

-----Original Message-----
From: (b)(6)
Sent: Thursday, January 28, 2010 9:37 AM
To: CSET
Subject: CSET

(b)(6)

Pages 16 through 18 redacted for the following reasons: Duplicate

Pages 19 through 27 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 28 through 35 redacted for the following reasons: Duplicate

AURORA Vulnerability

Mitigation Strategy

DRAFT v. 0.1

May 2, 2007

Pages 37 through 42 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 43 through 220 redacted for the following reasons: Duplicate

Control Systems Security

SHSGAC Brief

Homeland Security

Agenda

- Vulnerability
- Tiger Team
- Public Awareness
- Validation/Mitigation
- Mitigation Plan
- Knowledge Gap Assessment
- Control Systems Security Current Activities

Page 223 redacted for the following reason:

(b)(5), (b)(7)e, (b)(7)f

Aurora Vulnerability

- Equipment Necessary for an Attack
  - Programmable Digital Relay
  - High-Speed Breakers
  - Laptop/Desktop Computer
  - Synchronous electrical machines (generators, motors, pumps)
- Access required (front panel, modem, Internet, wireless, or SCADA)
- Knowledge Necessary to launch an attack:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)

Tiger Team

- Formed under direction from U/S Foresman
- Tiger Team goals:
  - Scope the vulnerability, threat, and risk of the Aurora scenario
  - Execute validation test and evaluate results
  - Develop mitigation strategy as needed
- Tiger Team members include representatives of DHS, DOE, DOD, FERC, NRC, FBI, DOS, Treasury, and EPA
- Tiger Team is coordinating with representatives from private industry
  - North American Electrical Reliability Corporation (NERC)
  - Tennessee Valley Authority
  - Electric Sector Coordinating Council
  - Nuclear Sector Coordinating Council

Public Awareness

- General public awareness seems imminent and could increase the level of threat
  - House Homeland Security Subcommittee on Emerging Threats and Cyber Security has made a request to tour the INL
  -

(b)(5), (b)(7)f

- Florida State University has published a white paper on the general subject of attacking the power grid

Control Systems Security Current Activities

- DHS Federal Control Systems Security Working Group is developing the Federal Coordinating Strategy for Securing Control Systems to address cross-sector focus and guidance
- DoE through the National SCADA Test Bed and the Roadmap to Secure Control Systems in Energy Sector provide focus and guidance for the Energy Sector
- DHS/DoE Outreach and awareness to public and private sector through education, training, conferences, seminars, and the promotion of industry recommended practices
- DHS/DoE Performing equipment and systems vulnerability assessments and the support tools and technologies
- DoD strategically partnering with DHS, DoE, and other Federal agencies to protect the critical infrastructure of the Defense Industrial Base
- Educating the intelligence community on the indicators and warning of controls systems and SCADA attack scenarios

Homeland Security

Pages 229 through 231 redacted for the following reasons: Duplicate

Pages 232 through 234 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

SUMMARY OF CONCLUSIONS

A blank sheet of paper with the above header will be provided to enable the Secretary, Deputy Secretary, and other DHS participants to capture agreed upon outcomes of the meeting, including deliverables, expected next steps, and general follow-up. This is intended to be filled out during the meeting. For a meeting attended by Component representatives, Summary of Conclusions are due to ES 24 hours after the meeting -- appropriately cleared and approved by Component Head, Deputy, or Chief of Staff. Component Exec Sec must certify in the e-mail that forwards the Summary of Conclusions, which one of the three served as the approving authority.

Please do not attach to briefing memorandum submissions.

Pages 236 through 285 redacted for the following reasons: Duplicate

Pages 286 through 290 redacted for the following reasons: Referred

Pages 291 through 387 redacted for the following reasons: Duplicate

Pages 388 through 393 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 394 through 396 redacted for the following reasons: Duplicate

Pages 397 through 399 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 400 through 442 redacted for the following reasons: Duplicate

Pages 443 through 445 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Aurora Tiger Team

Requests to Industry and Way Ahead

April 4, 2007

Pages 447 through 449 redacted for the following reasons:

(b)(5), (b)(7)e, (b)(7)f

THIS PAGE INTENTIONALLY LEFT BLANK

Aurora Industry Technical Team Meeting

A small group of industry experts from electric and nuclear sectors met on Wednesday, April 25 in Chicago to discuss their industry data call results and mitigation measures. DHS and DoE participated in the meeting and highlights from the meeting follow:

- The electric and nuclear sectors send out a data call to their respective members in an effort to address the identified knowledge gaps
    - What types of relays are in the installed base?
    - What types of remote access exists to the relays?
- Two major conclusions were drawn by the group based on the results
    - There were more dial-up modems out there than expected.
    - The overwhelming majority of the relays out there are Schweitzer Engineering Laboratories (SEL) and the top three manufacturers are SEL, ABB, and GE.
- There was a review of the basic risk equation: Risk = (Threat * Vulnerability * Consequence). Consensus was that T was low, V was real but not fully quantified, and that C was potentially huge. Ordinarily, if any element is 0 then risk is 0. But, the consensus was that this is a problem that requires immediate action with a caveat that we need to think it through thoroughly enough to ensure we take the right action.
- After a thorough discussion of the vulnerability and a consensus understanding of the various ways it can manifest itself, there was a brain storming session on all the possible mitigations
    - Input was solicited from all electric and nuclear sector industry members at the table, Government representative, as well as National Lab staff
    - The output of the brain storming was captured in a document and will be shared with the Tiger Team after being vetted by the Aurora Industry Team
    - The mitigation ideas were grouped into short-term (30-60 days), mid-term (60-180 days), or long-term (greater than 180 days)
    - The technical vetting of the mitigation ideas captured will be complete by May 11, 2007.
    - Several of the mid- and long-term mitigations require engagement with the vendors and some of the possible mitigations that the group came up with seem relatively easy for the manufacturers to accomplish. But, the manufacturers must be brought in soon.
- One new idea presented was contingency planning. In other words, what would the response be if the worst case scenario happened? What would the National Response Planning-related implications possibly be?
- As soon as a draft mitigation plan is written and near completion it was suggested that the top three relay manufacturers are called to a meeting hosted by NERC and NEI to discuss the vulnerability, mitigation plan, and to solicit their ideas on the various mitigation proposals.

- The Aurora Industry Technical Team will hold weekly teleconferences to update progress and all members made a commitment to NERC and NEI to work this issue to completion so we have some continuity.
- NCSD will be briefing the Senate Homeland Security and Governmental Affairs Committee staff on Monday, April 30. DoD and DoE will also attend the briefing.
- It is expected that a principal's meeting with Ms. Townsend will be called around May 4 (end of next week or the beginning of following week) to present an update on current activities, next steps, and the draft mitigation plan. Neill from HSC will coordinate this event once that is scheduled.

4/17/2012

Aurora Mitigation Meeting Teleconference

Attendees:

Perry Pederson	DHS/NCSD
(b)(6)	NERC (E-SCC)
	(b)(6)
Jim Caverly	DHS/IP
(b)(6)	DoE/OE
	DHS/CNPPD
(b)(6)	(b)(6) contract support to INL)
	contract support to INL)

Pages 454 through 571 redacted for the following reasons: Duplicate

Pages 572 through 574 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 575 through 610 redacted for the following reasons: Duplicate

Pages 611 through 616 redacted for the following reasons: Referred

Pages 617 through 618 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 619 through 641 redacted for the following reasons: Duplicate

Pages 642 through 648 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 649 through 655 redacted for the following reasons: Duplicate

From: (b)(6)
Sent: Tuesday, April 24, 2007 4:39 PM
To: (b)(6) Pederson, Perry A
Subject: Draft Strawman for Industry discussions rev.doc

Attachments: Draft Strawman for Industry discussions rev.doc
Here is the strawman as it currently exists...wanted you to see it before I send it to the group.

Pages 657 through 658 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 659 through 664 redacted for the following reasons: Duplicate

Pages 665 through 666 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 667 through 668 redacted for the following reasons: Duplicate

Morning Session – 21 March 07

Fuel Supply - Risks

Power Plants - Risks

Transmission & Distribution - Risks

Load - Risks

(b)(5)

Defense Industrial Base – Special Mfg., Telecom, Petroleum Refining, HVAC

Impact: E. Tightly coupled spinning machinery

Pumps?

Refinery big concern. Physical damage to refineries.

Military Specific - Risks

(b)(5)

(b)(5), (b)(7)e, (b)(7)f

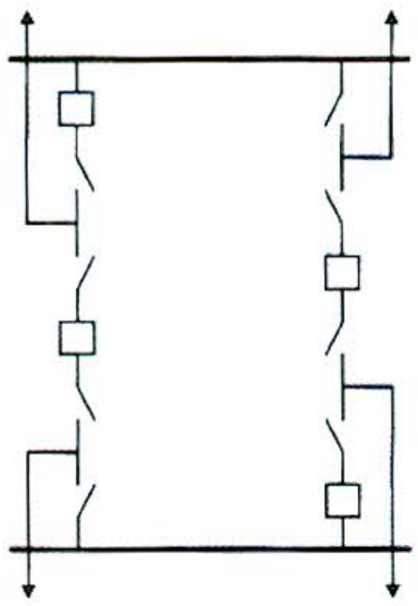
Pages 670 through 681 redacted for the following reasons: (b)(5), (b)(6), (b)(7)(c) (b)(7)(e), (b)(7)(f)

Pages 682 through 693 redacted for the following reasons: Duplicate

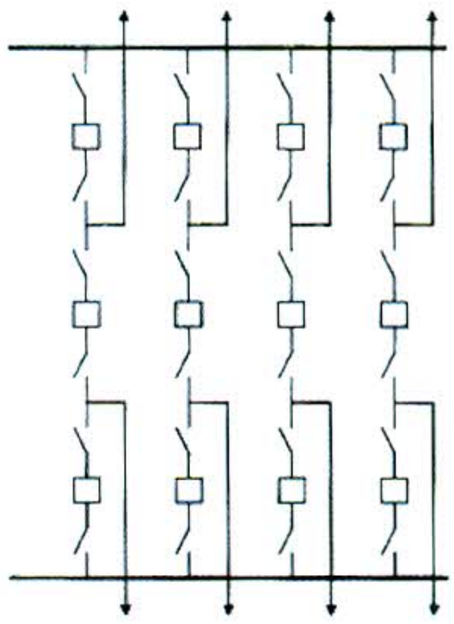
Pages 694 through 697 redacted for the following reasons: Referred

Discussion of Different Substation Configurations

With extra-high voltage (EHV) substations (345kV and above) it is common to see either a ring or breaker and a half substation configuration. Generally a ring bus is chosen if there fewer than four to six connections. These configurations have the advantage of facilitating operational flexibility than simpler radial bus connections. For example, any substation circuit breaker can be removed from service for maintenance without requiring a line to be de-energized. But these schemes require that two circuit breakers need to be opened to clear any fault on the line.



Example Ring Bus Substation Configuration



Example Breaker-and-a-Half Substation Configuration

Multifunction protective relays installed in the substation to provide line protection would normally be programmed and configured to isolate faults on the line it's protecting by commanding both circuit breakers connected to the line to open. ***Accessing a single protective relay would allow the line to be isolated..***

While not all reclosing schemes are designed the same (some operating philosophies permit automatic reclosing of both circuit breakers while others require manual reclosing of the second one), they generally identify a lead breaker to reclose first.[1]

While these substation configurations are more complex than simple radial systems, the complexity is addressed during the design, installation, and programming of the protective relay logic. Accessing and reprogramming a single protective relay would be sufficient to both completely isolate the line segment and command a reclose. Therefore, from the perspective of the adversary who is interested in exploiting this vulnerability, this additional complexity is of little or no concern (and represents no additional barrier to exploitation).

---

[1] http://www.nxtphase.com/pdfs/Ring%20Bus_2.pdf

Project Name: ***Aurora Generator Test***

Project Location: ***INL***
Estimate Number: ***9A17***

Project Summary Report

Client: ***L. E. Goldman, 6-0010***
Prepared By: ***R. R. Honsinger***
Estimate Type: ***Class 3***

Level	Description	Estimate Subtotal	Escalation	Contingency	Contingency %	TOTAL
	Project Management (PM)	$355,620	$0	$106,686	30.00%	$462,306
	. . . . BEA Project Management	$195,620	$0	$58,686	30.00%	$254,306
	. . . . Industrial Experts and Consultants	$160,000	$0	$48,000	30.00%	$208,000
	Generator Procurement	$371,000	$0	$18,550	5.00%	$389,550
	Site Assessment and Walk-down	$6,000	$0	$300	5.00%	$6,300
	System Engineering and Design	$86,942	$0	$26,083	30.00%	$113,024
	. . . . System Engineering and Design	$86,942	$0	$26,083	30.00%	$113,024
	Equipment Procurement	$85,560	$0	$64,170	75.00%	$149,730
	Construction and Installation	$309,086	$0	$87,869	28.43%	$396,956
	. . . . Construction - Pad and Barrier Construction	$156,224	$0	$31,245	20.00%	$187,468
	. . . . . General Conditions	$14,065	$0	$2,813	20.00%	$16,878
	. . . . . Sitework	$34,542	$0	$6,908	20.00%	$41,450
	. . . . . Concrete	$72,228	$0	$14,446	20.00%	$86,674
	. . . . . Masonry	$35,389	$0	$7,078	20.00%	$42,466
	. . . . Equipment Installation	$107,659	$0	$43,064	40.00%	$150,722
	. . . . . Mechanical - Subcontractor	$6,040	$0	$2,416	40.00%	$8,456
	. . . . . Install Generator Fuel and Cooling Systems	$6,040	$0	$2,416	40.00%	$8,456
	. . . . . Electrical - Subcontractor	$57,325	$0	$22,930	40.00%	$80,254
	. . . . . Install Diesel Generator	$15,885	$0	$6,354	40.00%	$22,238
	. . . . . Install Cable	$21,980	$0	$8,792	40.00%	$30,771
	. . . . . Remove Generator and Cable	$19,460	$0	$7,784	40.00%	$27,245
	. . . . . Electrical - BEA	$44,294	$0	$17,718	40.00%	$62,012
	. . . . . Hookups at Substation	$19,599	$0	$7,840	40.00%	$27,439
	. . . . . Install Test Equipment	$9,415	$0	$3,766	40.00%	$13,181
	. . . . . Install Video/TV Capture Equipment	$9,415	$0	$3,766	40.00%	$13,181

Project Summary Report

Project Name: ***Aurora Generator Test***

Project Location: ***INL***
Estimate Number: ***9A17***

Client: ***L. E. Goldman, 6-0010***
Prepared By: ***R. R. Honsinger***
Estimate Type: ***Class 3***

Level	Description	Estimate Subtotal	Escalation	Contingency	Contingency %	TOTAL
	Site Cleanup and Equipment Removal	$79,060	$0	$31,624	40.00%	$110,685
	. . . . Equipment Removal Site Restoration	$79,060	$0	$31,624	40.00%	$110,685
	. . . . . Remove Generator and Cable	$29,460	$0	$11,784	40.00%	$41,245
	. . . . . Remove Blocks and Conc Pad	$30,000	$0	$12,000	40.00%	$42,000
	. . . . . Environmental and WGS Support	$19,600	$0	$7,840	40.00%	$27,440
	BEA Material Handling Fee and G&A	$66,750	$0	$6,675	10.00%	$73,425
	Work For Others (WFO) Fees	$63,000	$0	$18,900	30.00%	$81,900
Total	Aurora Generator Test	$2,187,038	$0	$689,771	31.54%	$2,876,809

Page 701 was blank and removed

Pages 702 through 707 redacted for the following reasons: (b)(5), (b)(6), (b)(7)(c) (b)(7)(e), (b)(7)(f)

Pages 708 through 715 redacted for the following reasons: Duplicate

GAO Control Systems Review 310841

Requested Documents

1. CS Analyst Handbook/SOP (with flow chart)
2. Cyber Incidents Involving Control Systems (KEMA/BCIT incident databases)
3. Site Assessment Templates
4. DHS/CSSP and DoE/NSTB Vendor Assessment Matrix
5. INL 2007 Annual Work Plan
6. Summary of CS Efforts by Industry (post-assessment actions by industry)
7. Contract and SOW with Noblis for PCSF
8. CSSC Methodology for Vulnerability Assessments

Path to the above documents and this document:
L:\Control Systems Security Program\Working Files\NCSD Tasker Responses\GAO\GAOrequesteddocs9May07

Requested FOUO Documents

10. Aurora Briefing
11. Nuclear Plant Scenario
12. Induction Motor Scenario
13. Cyber Security Assessment Report: Bureau of Reclamation - Central Valley Operations

Page 717 redacted for the following reasons: (b)(5), (b)(6), (b)(7)(c) (b)(7)(e), (b)(7)(f)

Pages 718 through 724 redacted for the following reasons: Duplicate

Pages 725 through 771 redacted for the following reasons: Duplicate

Pages 772 through 773 redacted for the following reasons: (b)(5), (b)(6), (b)(7)(c) (b)(7)(e), (b)(7)(f)

Pages 774 through 781 redacted for the following reasons: Duplicate

U5 Aurora Contacts for CSSP

(b)(6), (b)(7)c

Pages 783 through 784 redacted for the following reasons: (b)(5), (b)(7)(e), (b)(7)(f)

Pages 785 through 802 redacted for the following reasons: Duplicate

(b)(6)

From: (b)(6), (b)(7)c
Sent: Friday, September 07, 2007 6:21 PM
To:
Cc: (b)(6), (b)(7)c
Subject: Control Systems - Media Advisory
Attachments: Control Systems Vulnerability PAG QandAs 20070822 v01 FINAL.zip

Dear (b)(6)

Per my voice mail, we wanted to get in touch with you regarding an important heads up with respect to a potential forthcoming news story regarding a control systems vulnerability.

We would like to discuss this with you and hope that we can connect on Monday. Please let us know when you might have some availability. We have included public affairs guidance we prepared for your consideration.

Thank you,

(b)(6)

(b)(6), (b)(7)c
National Cyber Security Division
U.S. Department of Homeland Security
Tel: (b)(6), (b)(7)c

(b)(6)

From: (b)(6), (b)(7)c
Sent: Friday, September 07, 2007 6:07 PM
To:
Cc: (b)(6), (b)(7)c
Subject: RE: Public Affairs Guidance

Dea (b)(6)

The password for the attached file is: (b)(5)

Thank you,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Friday, September 07, 2007 6:07 PM
To
Cc (b)(6), (b)(7)c
Subject: Public Affairs Guidance

Dear(b)(6), (b)(7)c

Per our discussion earlier today, attached please find the public affairs guidance for your consideration.

I look forward to hearing from you on the other topic as well.

Please let us know if you have any questions.

Thank you,
(b)(6), (b)(7)c

(b)(5), (b)(7)c
National Cyber Security Division
U.S. Department of Homeland Security
Tel: (b)(6), (b)(7)c

Pages 805 through 812 redacted for the following reasons: Duplicate

Pages 813 through 820 redacted for the following reasons: (b)(5), (b)(6), (b)(7)(c) (b)(7)(e), (b)(7)(f)