I3P INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION

Building a Digital Commons of Cyber Security Resources

7th International Conference on Grey Literature

Nancy, France

December 5-6, 2005

Patricia Erwin

perwin@thei3p.org

Overview of the Institute for Information Infrastructure Protection

The Cyber Security Digital Commons is a project sponsored by the Institute for Information Infrastructure Protection (I3P) located at Dartmouth College, Hanover NH.

- Funding for the I3P comes from the US Department of Homeland Security (DHS) and the National Institute for Science and Technology (NIST)

- The I3P Consortium is composed of US academic institutions, national labs, and not-for-profit research organizations – all have strong cyber security research programs or focus.

- The I3P Consortium sponsors research projects and programs.

- The Cyber Security Digital Commons is a project that includes both public and private information tools and services.

Digital Commons of Cyber Security Resources

Mission

We seek to be the electronic conduit through which users learn, collaborate, and create new knowledge in the broad area of information infrastructure protection. Our unique approach will be the emphasis on scope, making it the first place the cyber security community [and others] turn to for what is happening in the world of information infrastructure protection.

Tools and Services

- International Calendar of Cyber Security Events
- Funding Opportunities in Cyber Security
- Security in the News
- International Cyber Security Organization Directory
- Cyber Security Glossary and Taxonomy
- Cyber Security Digital Library

Cyber Security Digital Library

Scheduled to open to the public on February 1, 2006

- 25+ types of information identified in the digital library.
- Uses modified version of the Dublin Core for meta-record creation.
- Resources come from our members, are produced internally, and are identified from a variety of outside sources.
- Access to resources is controlled at the document level.

My primary focus for today is on the grey literature in cyber security

- Not previously published through the standard publication processes.
- In a variety of formats and conditions.
- May have use restrictions.
- Authorship and/or ownership may be unclear.
- Research value may be unclear – hard to predict for the future.

Grey Literature in Cyber Security – the Challenges

There are social, legal, and logistical challenges to acquiring or providing access to grey literature in cyber security.

Social

- Culture of informality
- Machines can manage our information
- Data is often hard to get precisely because it has intentionally not been captured
- Informal publishing model – not everyone is an academic
- Sustainability – our funding ends in 2007

Legal challenges are particularly daunting

- Copyright
- Nondisclosure agreements
- US export control laws
- US Freedom of Information Act

Logistics

- As an academic discipline not that old
- Where are the ‘pockets’ of information

Challenges Related to the Resources

- **Location** – how do we identify where the pockets of resources are hidden?

- **Access** – Once the pockets have been identified, how easily can we access the resources for cataloging and digitalization? Roving bands of catalogers might be needed.

- **Verification and authentication** – How do we know the information is useful and truly what it says it is?

- **Permanence of location** – Since we will be linking to the majority of these resources, how do we know their location will remain permanent?

- **Long term preservation** – Since we are not providing stewardship over the resources, how do we know that they will be preserved for future use?

Grey Literature Resources We Are Most Interested in Capturing

Expertise Notes

Presentations

Industry Notes

Product Reviews

Policies & Procedures

Best Practices

Consortium Decisions

Researcher Notes

Research Data

Trip Reports

Workshop Findings

Foundation Documents

Planning Documents

Collection Development

Policy

Meta-record created about the resource

Resource is secured in the Digital Repository, if I3P has stewardship over the resource

Access code in meta-record determines who can see the resource

Searchable Meta-record is accessible to the public

Typical Meta-record (simplified) for a Resource –user view, showing search, browse, authority control

Title: I3P Trip report for NPRA **(S, B)**

Author: Benjamin Cook **(S, A)**

Date: [November 2, 2005]

Description: Trip report filed after attending National Petrochemical and Refiners Association 2005 Technical Forum in Grapevine, TX , on October 19-20. Ben Cook (Sandia Nat. Lab) and Ulf Lindqvist (SRI International) represented the I3P. **(S)**

Abstract: We were invited by _____ of ___ Refining to present an update on our I3P project in the Plant Automation session. The majority of attendees were refinery operators and managers with the remainder being service and equipment vendors representing all aspects of refining. There seems to be a growing concern about cyber security issues, but more awareness building is necessary and this appears to be an area where our I3P efforts can really make an immediate difference. **(S)**

Type: Trip report **(S, B)**

Keywords: Oil refining; security issues; refineries; alarm management; oil supply **(S, B)**

URL: [url hidden to non-authorized viewers]

Access Rights: Viewable by Consortium members and SCADA researchers

Rights Holder: I3P **(B)**

Contact Information

To learn more about the I3P Digital Commons of Cyber Security Resources, please contact:

Patricia Erwin
Senior Assistant Director, Institute for Information Infrastructure Protection
Dartmouth College
45 Lyme Rd.
Hanover, New Hampshire 03755
(603) 646-0650
perwin@thei3p.org