Cooperative Protection Program (CPP) Status FY10

Jeff Mauth

Project Manager

May 19, 2010

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Agenda

- Sensor Integration
- Sensor Deployment
- CPP Portal
- Mercury
- Parting Comments
- Questions

Sensor Integration

Task Lead: Greg Thomas

- Flo and Flower: Session Data
- Snort: Network Intrusion Detection Data
- AMP: Various Types of Network Data
- PopQuiz: Various Types of Network Data
- T3: Data Movement and Sensor Control

Sensor Deployment

Task Lead: Liz Faultersack

- Certification and Accreditation
- Continued Expansion
- Hardware Refresh to Begin FY11

CPP Portal

Task lead: Brett Didier

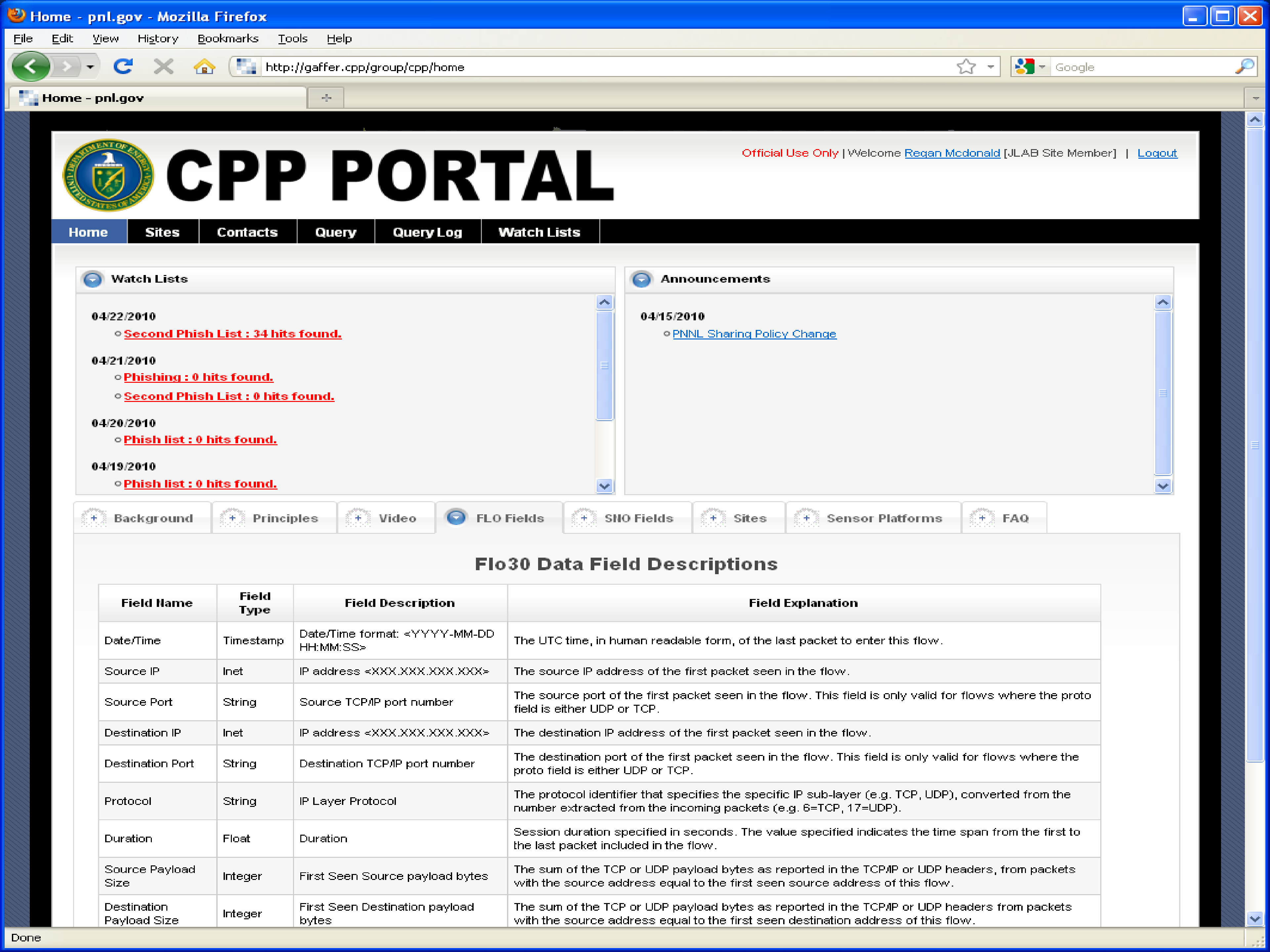
- Features
- Sharing Policy
- Data and Releases

CPP Portal

- Provides DOE cyber analysts access to CPP collected “DOE enterprise” data
- Implements “glass house” approach for data access
- Promotes cross-site sharing and collaboration
- Interested? Talk to us or email cpp.portal@pnl.gov.

Sharing Policy – You get what you give

		Sharing Policy of Sites Being Queried		
		Anonymous	Summary	Detail
Sharing Policy for Site Performing Query	Detail	Will see anonymous aggregate for the sites that chose this option. Cannot query against IP address space of Anonymous sites.	Will see summary line for the sites that chose this option.	Will see summary line and can view/download detail results for the sites that chose this option.
	Summary	Will see anonymous aggregate for the sites that chose this option. Cannot query against IP address space of Anonymous sites.	Will see a summary line for each site that chose Summary or Detail.	
	Anonymous	Will see single summary line that is an anonymous aggregate for all sites. Cannot make queries against any DOE IP address space.		



CPP PORTAL

Official Use Only | Welcome Regan Mcdonald [JLAB Site Member] | Logout

Watch Lists

04/22/2010

- Second Phish List : 34 hits found.

04/21/2010

- Phishing : 0 hits found.
- Second Phish List : 0 hits found.

04/20/2010

- Phish list : 0 hits found.

04/19/2010

- Phish list : 0 hits found.

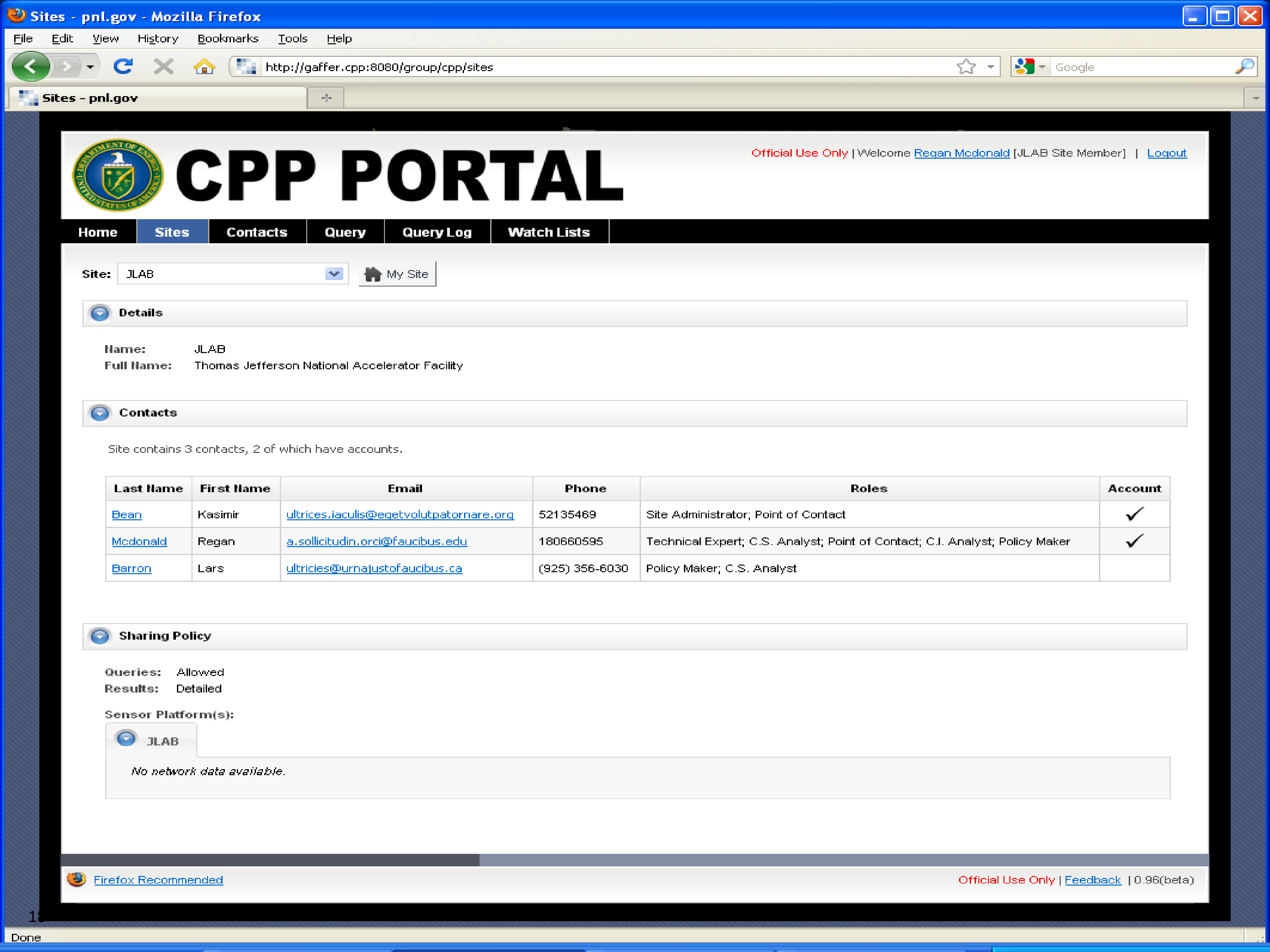
Announcements

04/15/2010

- PNNL Sharing Policy Change

Flo30 Data Field Descriptions

Field Name	Field Type	Field Description	Field Explanation
Date/Time	Timestamp	Date/Time format: <YYYY-MM-DD HH:MM:SS>	The UTC time, in human readable form, of the last packet to enter this flow.
Source IP	Inet	IP address <XXX.XXX.XXX.XXX>	The source IP address of the first packet seen in the flow.
Source Port	String	Source TCP/IP port number	The source port of the first packet seen in the flow. This field is only valid for flows where the proto field is either UDP or TCP.
Destination IP	Inet	IP address <XXX.XXX.XXX.XXX>	The destination IP address of the first packet seen in the flow.
Destination Port	String	Destination TCP/IP port number	The destination port of the first packet seen in the flow. This field is only valid for flows where the proto field is either UDP or TCP.
Protocol	String	IP Layer Protocol	The protocol identifier that specifies the specific IP sub-layer (e.g. TCP, UDP), converted from the number extracted from the incoming packets (e.g. 6=TCP, 17=UDP).
Duration	Float	Duration	Session duration specified in seconds. The value specified indicates the time span from the first to the last packet included in the flow.
Source Payload Size	Integer	First Seen Source payload bytes	The sum of the TCP or UDP payload bytes as reported in the TCP/IP or UDP headers, from packets with the source address equal to the first seen source address of this flow.
Destination Payload Size	Integer	First Seen Destination payload bytes	The sum of the TCP or UDP payload bytes as reported in the TCP/IP or UDP headers from packets with the source address equal to the first seen destination address of this flow.



Sites - pnl.gov - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://gaffer.cpp:8080/group/cpp/sites
Google
Sites - pnl.gov

CPP PORTAL

Official Use Only | Welcome Regan Mcdonald [JLAB Site Member] | Logout

Site: JLAB

Details

Name: JLAB
Full Name: Thomas Jefferson National Accelerator Facility

Contacts

Site contains 3 contacts, 2 of which have accounts.

Last Name	First Name	Email	Phone	Roles	Account
Bean	Kasimir	ultrices.iaculis@egetvolutpatornare.org	52135469	Site Administrator; Point of Contact	✓
Mcdonald	Regan	a.sollicitudin.orci@faucibus.edu	180660595	Technical Expert; C.S. Analyst; Point of Contact; C.I. Analyst; Policy Maker	✓
Barron	Lars	ultricies@urnajustofaucibus.ca	(925) 356-6030	Policy Maker; C.S. Analyst	

Sharing Policy

Queries: Allowed
Results: Detailed

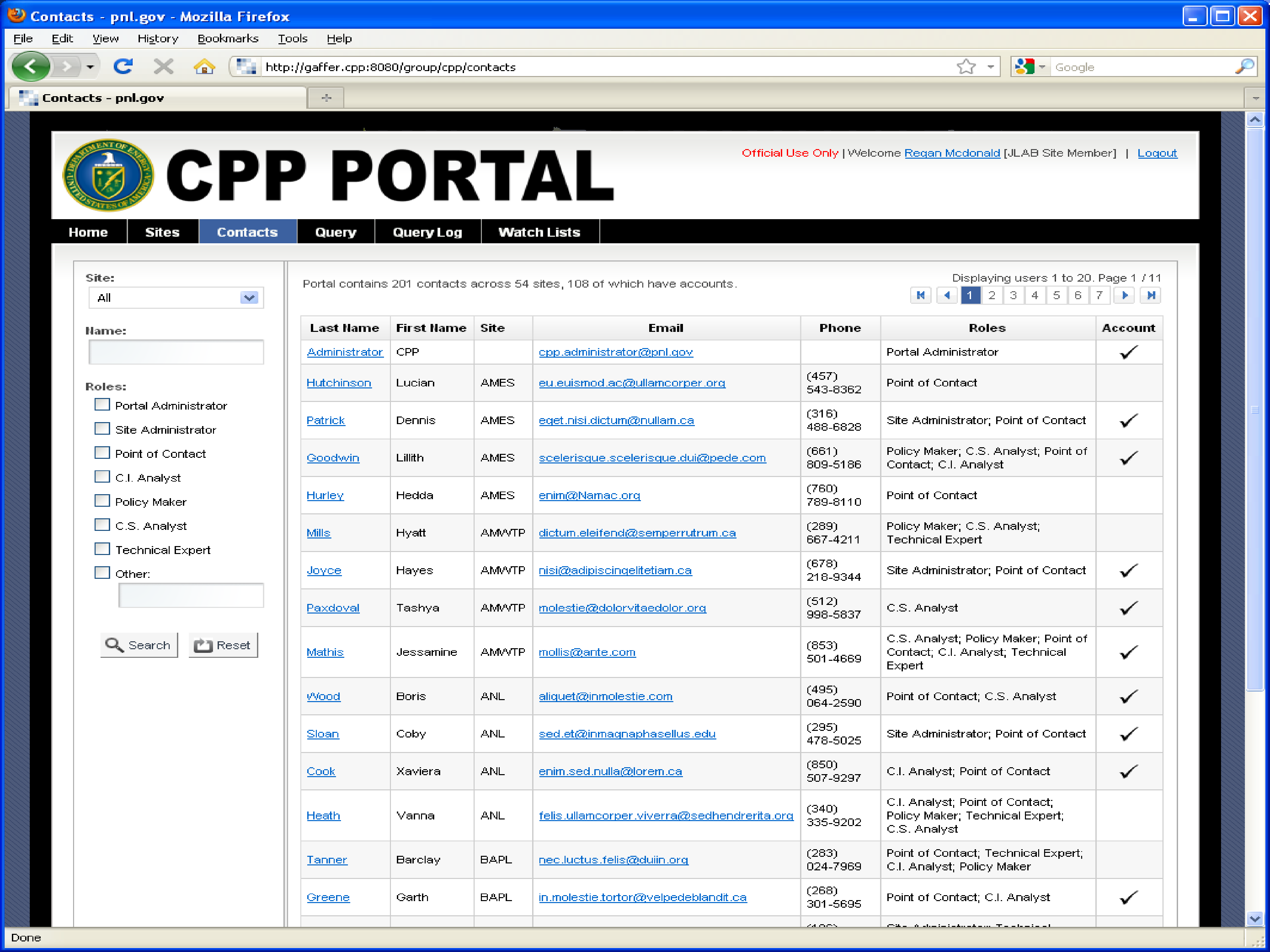
Sensor Platform(s):

JLAB

No network data available.

Firefox Recommended

Official Use Only | Feedback | 0.96(beta)



Official Use Only | Welcome Regan Mcdonald [JLAB Site Member] | Logout

Site: All

Name:

Roles:

□ Portal Administrator

□ Site Administrator

□ Point of Contact

□ C.I. Analyst

□ Policy Maker

□ C.S. Analyst

□ Technical Expert

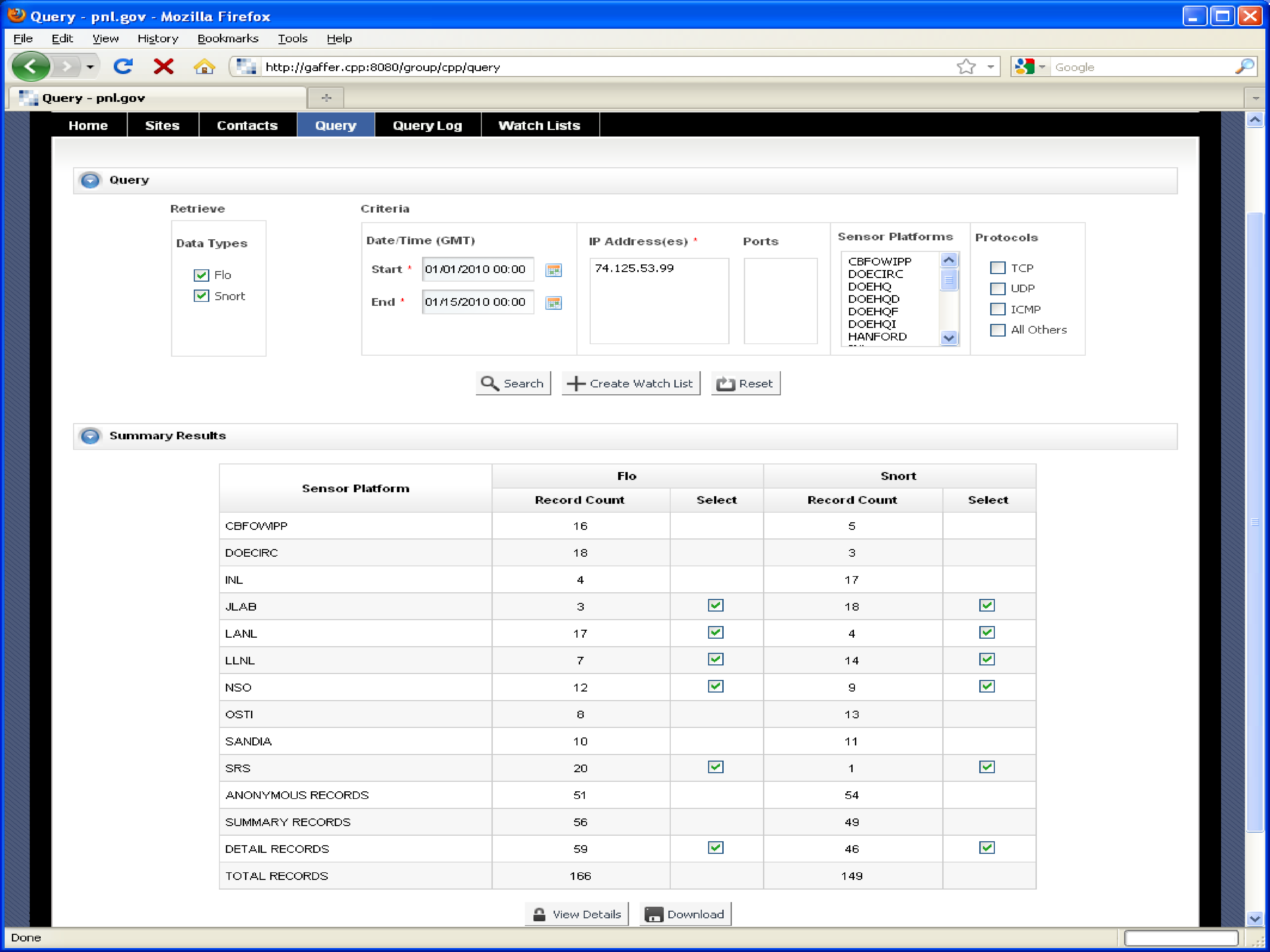
□ Other:

Portal contains 201 contacts across 54 sites, 108 of which have accounts.

Displaying users 1 to 20. Page 1 / 11

1 2 3 4 5 6 7

Last Name	First Name	Site	Email	Phone	Roles	Account
Administrator	CPP		cpp.administrator@pnl.gov		Portal Administrator	✓
Hutchinson	Lucian	AMES	eu.euismod.ac@ullamcorper.org	(457) 543-8362	Point of Contact	
Patrick	Dennis	AMES	eget.nisi.dictum@nullam.ca	(316) 488-6828	Site Administrator; Point of Contact	✓
Goodwin	Lillith	AMES	scelerisque.scelerisque.dui@pede.com	(661) 809-5186	Policy Maker; C.S. Analyst; Point of Contact; C.I. Analyst	✓
Hurley	Hedda	AMES	enim@Namac.org	(760) 789-8110	Point of Contact	
Mills	Hyatt	AMWTP	dictum.eleifend@semperrutrum.ca	(289) 667-4211	Policy Maker; C.S. Analyst; Technical Expert	
Joyce	Hayes	AMWTP	nisi@adipiscingelitetiam.ca	(678) 218-9344	Site Administrator; Point of Contact	✓
Paxdoval	Tashya	AMWTP	molestie@dolorvitaedolor.org	(512) 998-5837	C.S. Analyst	✓
Mathis	Jessamine	AMWTP	mollis@ante.com	(853) 501-4669	C.S. Analyst; Policy Maker; Point of Contact; C.I. Analyst; Technical Expert	✓
Wood	Boris	ANL	aliquet@inmolestie.com	(495) 064-2590	Point of Contact; C.S. Analyst	✓
Sloan	Coby	ANL	sed.et@inmagnaphasellus.edu	(295) 478-5025	Site Administrator; Point of Contact	✓
Cook	Xaviera	ANL	enim.sed.nulla@lorem.ca	(850) 507-9297	C.I. Analyst; Point of Contact	✓
Heath	Vanna	ANL	felis.ullamcorper.viverra@sedhendrerita.org	(340) 335-9202	C.I. Analyst; Point of Contact; Policy Maker; Technical Expert; C.S. Analyst	
Tanner	Barclay	BAPL	nec.luctus.felis@duiin.org	(283) 024-7969	Point of Contact; Technical Expert; C.I. Analyst; Policy Maker	
Greene	Garth	BAPL	in.molestie.tortor@velpedeblandit.ca	(268) 301-5695	Point of Contact; C.I. Analyst	✓



Query

Retrieve

Data Types

☑ Flo

☑ Snort

Criteria

Date/Time (GMT)

Start * 01/01/2010 00:00

End * 01/15/2010 00:00

IP Address(es) * 74.125.53.99

Ports

Sensor Platforms

CBFOWIPP
DOECIRC
DOEHQ
DOEHQD
DOEHQF
DOEHQI
HANFORD

Protocols

□ TCP

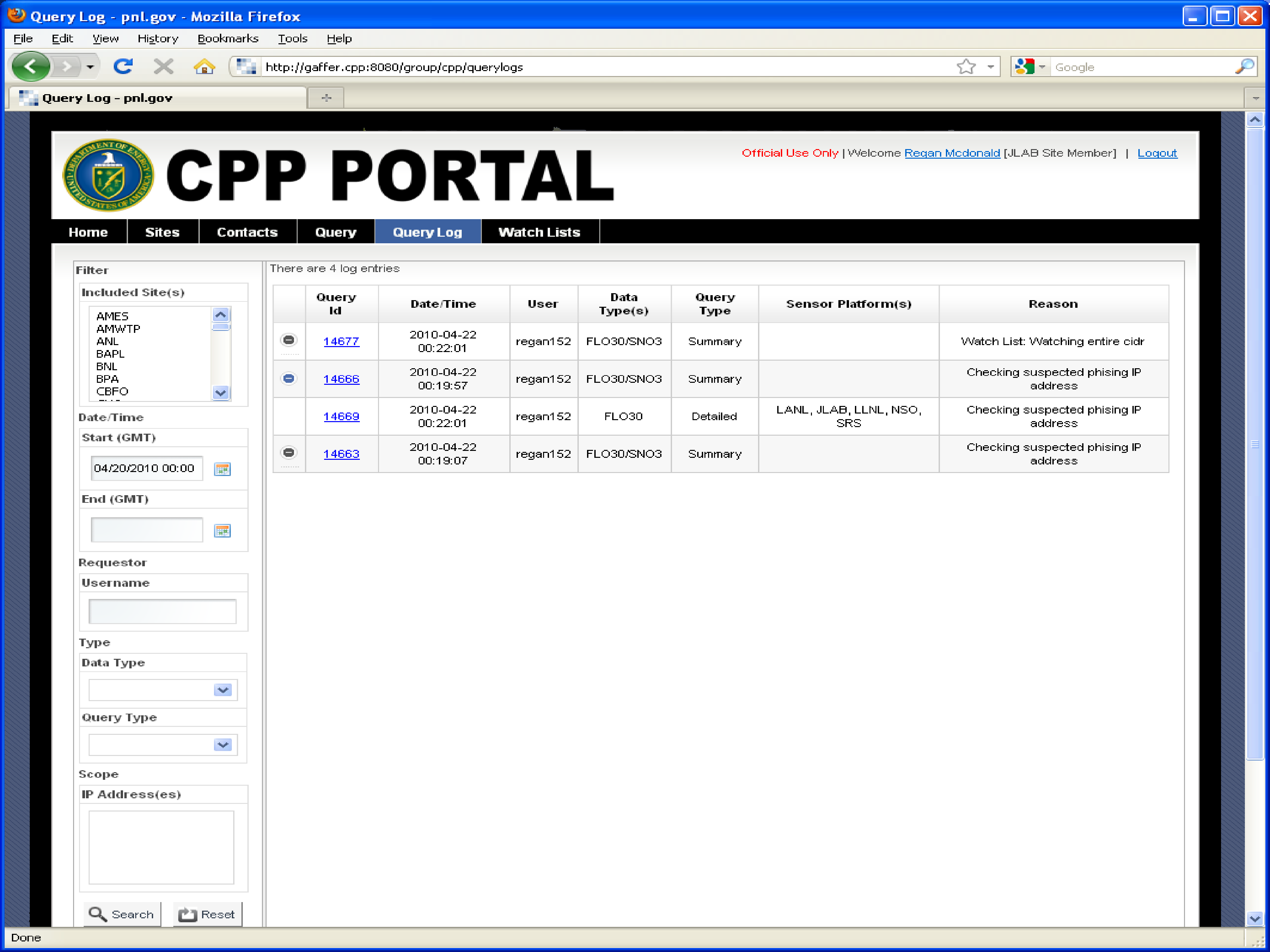
□ UDP

□ ICMP

□ All Others

Summary Results

Sensor Platform	Flo		Snort	
	Record Count	Select	Record Count	Select
CBFOWIPP	16		5	
DOECIRC	18		3	
INL	4		17	
JLAB	3	☑	18	☑
LANL	17	☑	4	☑
LLNL	7	☑	14	☑
NSO	12	☑	9	☑
OSTI	8		13	
SANDIA	10		11	
SRS	20	☑	1	☑
ANONYMOUS RECORDS	51		54	
SUMMARY RECORDS	56		49	
DETAIL RECORDS	59	☑	46	☑
TOTAL RECORDS	166		149	



Official Use Only | Welcome Regan Mcdonald [JLAB Site Member] | Logout

Filter

Included Site(s)

AMES
AMWTP
ANL
BAPL
BNL
BPA
CBFO

Date/Time

Start (GMT)

04/20/2010 00:00

End (GMT)

Requestor

Username

Type

Data Type

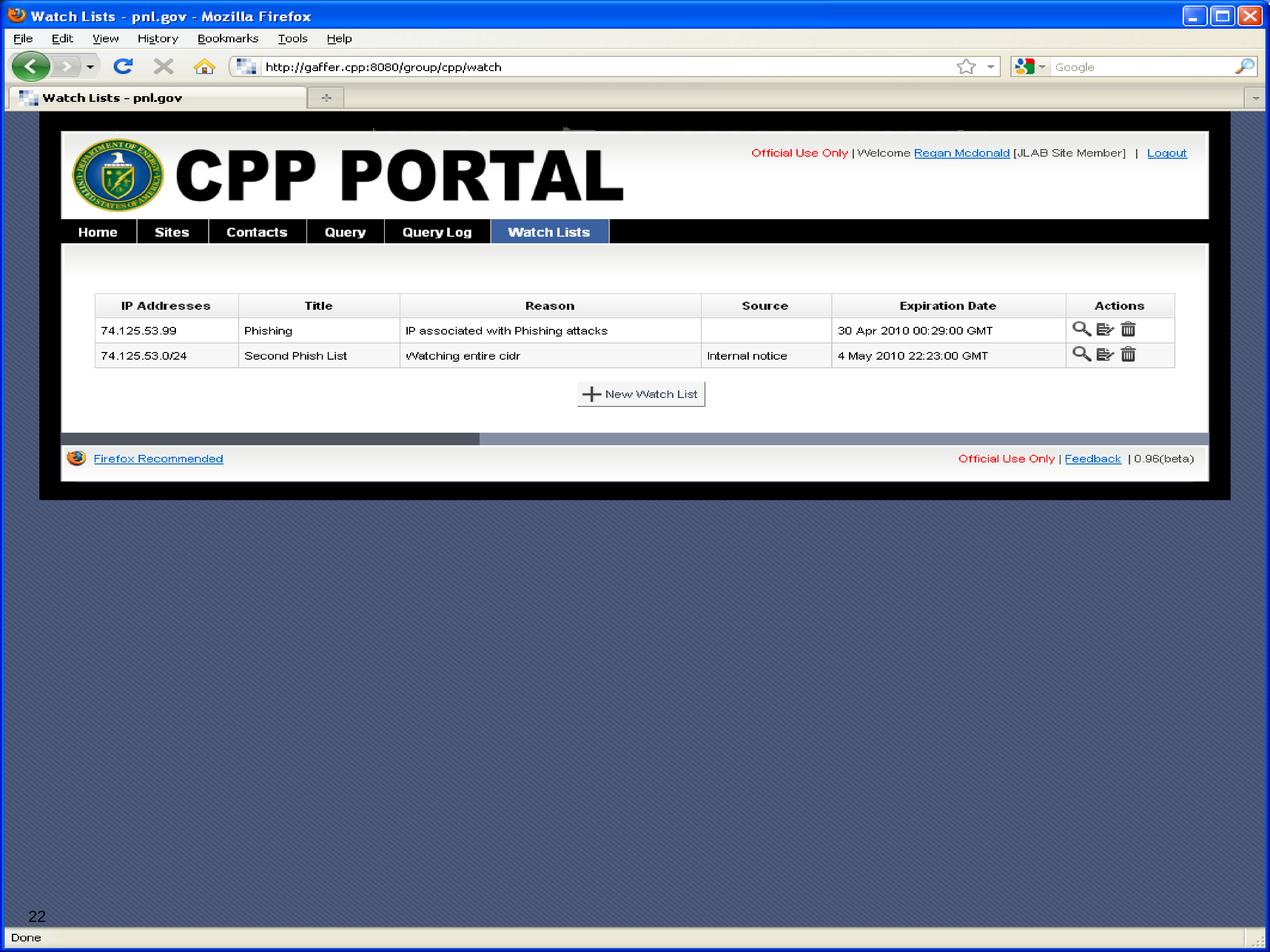
Query Type

Scope

IP Address(es)

There are 4 log entries

	Query Id	Date/Time	User	Data Type(s)	Query Type	Sensor Platform(s)	Reason
⊖	14677	2010-04-22 00:22:01	regan152	FLO30/SNO3	Summary		Watch List: Watching entire cidr
⊖	14666	2010-04-22 00:19:57	regan152	FLO30/SNO3	Summary		Checking suspected phising IP address
	14669	2010-04-22 00:22:01	regan152	FLO30	Detailed	LANL, JLAB, LLNL, NSO, SRS	Checking suspected phising IP address
⊖	14663	2010-04-22 00:19:07	regan152	FLO30/SNO3	Summary		Checking suspected phising IP address


Watch Lists - pnl.gov - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://gaffer.cpp:8080/group/cpp/watch
Google
Watch Lists - pnl.gov
Home
Sites
Contacts
Query
Query Log
Watch Lists
New Watch List
Done

CPP PORTAL

Official Use Only | Welcome Regan Mcdonald [JLAB Site Member] | Logout

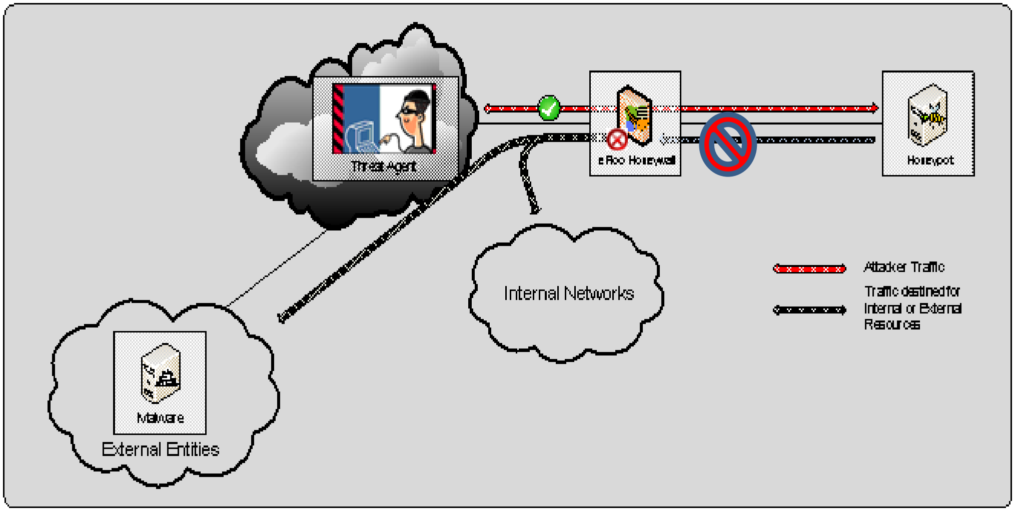
IP Addresses	Title	Reason	Source	Expiration Date	Actions
74.125.53.99	Phishing	IP associated with Phishing attacks		30 Apr 2010 00:29:00 GMT	🔍 📝 🗑
74.125.53.0/24	Second Phish List	Watching entire cidr	Internal notice	4 May 2010 22:23:00 GMT	🔍 📝 🗑

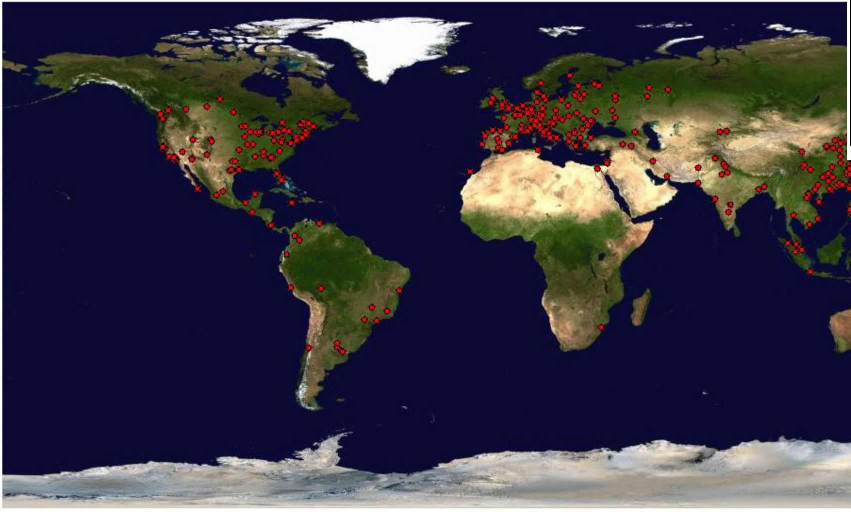
Firefox Recommended

Official Use Only | Feedback | 0.96(beta)

Mercury

- Deceptive Network Approach
- Deceptive Environment
- Analysis and Reporting





Parting Comments

- The cyber security capabilities in DOE are impressive.
- Trust is hard to gain but easy to loose.
- To counter the evolving threat we all need to work towards enabling:
  - Real time collaboration
  - Data sharing
  - Knowledge sharing
  - Framework to manage trust
  - Protected communications
- Communication and collaboration between everyone is key

Comments & Questions

Jeff Mauth
CPP Project Manager

Jeff.Mauth@pnl.gov

509-375-2511

Liz Faultersack
CPP Deputy Project Manager

Liz.F@pnl.gov

509-375-6408

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*