

Group B

FOIA/PA NO: 2014-0068

RECORDS BEING RELEASED IN PART

Pursuant to the requirements of *Vaughn v. Rosen*¹, the following types of information are being withheld:

- Ex. 3: Information about the design, manufacture, or utilization of nuclear weapons
 Information about the protection or security of reactors and nuclear materials
 Contractor proposals not incorporated into a final contract with the NRC
 Other _____
- Ex. 4: Proprietary information provided by a submitter to the NRC
 Other _____
- Ex. 5: Draft documents (D.P. Privilege)
 Correspondence deliberating a proposed action (D.P. Privilege)
 Records prepared by counsel in anticipation of litigation (A.W.P. Privilege)
 Privileged communications between counsel and a client (A.C. Privilege)
 Other _____
- Ex. 6: Agency employee PII, including SSN, contact information, birthdates, etc.
 Third party PII, including names, phone numbers, or other identifying information
- Ex. 7(A): Copies of ongoing investigation case files, exhibits, notes, ROI's, etc.
 Records that reference or are related to a separate ongoing investigation(s)
- Ex. 7(C): Special Agent or other law enforcement PII
 PII of third parties referenced in records compiled for law enforcement purposes
- Ex. 7(D): Witnesses' and Allegers' PII in law enforcement records
 Confidential Informant or law enforcement information provided by other entity
- Ex. 7(E): Law Enforcement Technique/Procedure used for criminal investigations
 Technique or procedure used for security or prevention of criminal activity
- Ex. 7(F): Information that could aid a terrorist or compromise security
 Retired Law Enforcement personnel
 Witnesses or unknown individuals who have participated in enforcement activity

Other/Comments: _____

¹ *Vaughn v. Rosen*, 484 F.2d 820, 827 (D.C. Cir. 1973), cert. denied, 415 U.S. 977 (1974); See also, *Mead Data Central, Inc. v. United States Department of the Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977) (encouraging agencies to provide requesters "with sufficient detail about the nature of the withheld documents and its exemption claims at the administrative level").

Harrington, Holly

From: Graham, Thorne
Sent: Wednesday, June 12, 2013 3:35 PM
To: Harrington, Holly
Subject: Fw: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx

Holly,

I miss poke. No need to review. Just FYI. Thank you for offering to assist.
Thorne Graham

From: Webber, Robert
To: Rich, Thomas; McCarthy, James; Paradiso, Karen; Graham, Thorne
Cc: Feibus, Jonathan; Offutt, David; Chew, Elizabeth; Gareri, Mario; Bladey, Cindy
Sent: Wed Jun 12 14:08:10 2013
Subject: RE: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx

Team:

Karen and I were happy to help last night but I suggest you send to ADM to post through the Agency Announcement system. Cindy Bladey is the ADM contact and helped us out last night.

Bob

From: Rich, Thomas
Sent: Wednesday, June 12, 2013 1:50 PM
To: McCarthy, James; Paradiso, Karen; Webber, Robert; Graham, Thorne
Cc: Feibus, Jonathan; Offutt, David; Chew, Elizabeth; Gareri, Mario
Subject: Re: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx

All,

Looks good. Couple of minor corrections needed:
- correct the contact paragraph - duplicate "please contact the..."
- remove Thorne and Computer office

Tom

From: McCarthy, James
To: Paradiso, Karen; Webber, Robert; Rich, Thomas; Graham, Thorne
Cc: Feibus, Jonathan; Offutt, David; Chew, Elizabeth; Gareri, Mario
Sent: Wed Jun 12 13:39:00 2013
Subject: RE: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx

That is the hope here, as quickly and visibly as possible.

Jim McCarthy
US Nuclear Regulatory Commission
Computer Security Office
Office: 301-415-5871
Mobile: (b)(6)

From: Paradiso, Karen
Sent: Wednesday, June 12, 2013 1:33 PM
To: McCarthy, James; Webber, Robert; Rich, Thomas; Graham, Thorne
Cc: Feibus, Jonathan; Offutt, David; Chew, Elizabeth; Gareri, Mario
Subject: RE: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx

Hi Jim,

Are you going to have this distributed via ADM's Announcement System?

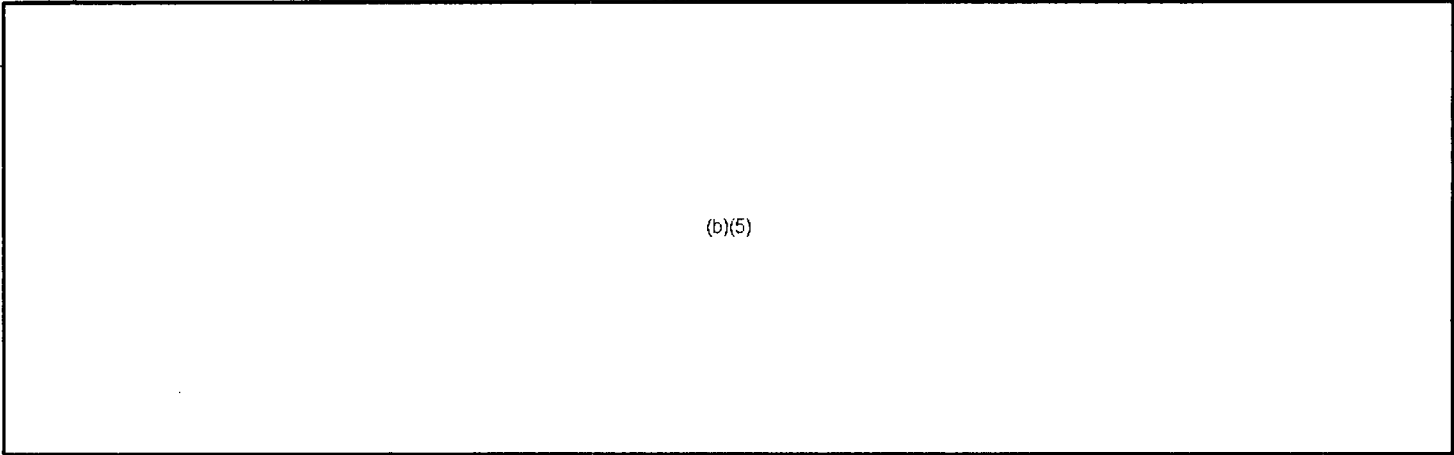
Thanks!
Karen

From: McCarthy, James
Sent: Wednesday, June 12, 2013 1:31 PM
To: Webber, Robert; Paradiso, Karen; Rich, Thomas; Graham, Thorne
Cc: Feibus, Jonathan; McCarthy, James
Subject: Final Revision: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx
Importance: High

All,

Final revised announcement content is below and attached. Please expedite the distribution of this announcement over e-mail and modify if you deem appropriate.

(b)(5)



(b)(5)

Thank you,
Jim McCarthy
US Nuclear Regulatory Commission
Computer Security Office
Office: 301-415-5871
Mobile: (b)(6)

From: Graham, Thorne
Sent: Wednesday, June 12, 2013 11:41 AM
To: McCarthy, James
Subject: Notice-Avoidance of Viewing Sensitive or Classified documents in the Public Domain- NSA.docx
Importance: High

Jim,

I was working on this while your message came in. Please review both and consolidate into a single message, keeping it down to one page. Thanks, Thorne

Information System Security Officer Forum Meeting

1/5/2011 1:00 – 2:00 PM

T8-A01

Dial-in #: 1-888-390-1012, Pass code:

(b)(6)

bl

Meeting called by:

(b)(6) Chief
Information Security Officer
(CISO), ISSO Forum Chair

Type of meeting:

Information, Discussion, &
Decisions

Requested Attendees:

Office ISSOs, CSO SITSOs

Please read:

Please bring: N/A

Agenda

ISSO Forum welcome

1:00-1:05

Computer security policy, standards, guidance, and training update

1:05-1:25

- Commercial role-based training
- FAA IT/ISS Conference

FISMA compliance update

1:25-1:30

Computer security situational awareness update

(b)(6)

1:30-1:50

- Wikileaks
- Cyber Assessment Team (CAT)
- Incident Response Database

ISSO Forum decisions

1:50-1:55

Wrap up/next steps/action item review

1:55-2:00

Next Meeting: February 8, 1:00-2:00pm, room T-8A01

Forum decisions needed on the following items:

FYI: For those that attend the forum via VTC or phone, please send an email to Judy.Petsch@nrc.gov to acknowledge your attendance. Confusion can occur at the start of the meeting which may prevent your attendance being recorded at that time. CSO would like to assure attendance credit for all.

bl

Information Systems Security Officer (ISSO) Forum Minutes
 1/5/2011, 1:00-2:00pm, T-8-A01

Office	ISSO Forum Member	Meeting Attendees
ACRS		
ADM		
ASLBP		
CSO		
FSME		
HR		
NMSS		
NRO		
NRR		
NSIR		
OCFO	(b)(6)	
OE		
OI		
OIG		
OIS		
RES		
R-I		
R-II		
R-III		
R-IV		
SBCR		
SECY		

66

Topics

The chair provided a New Year welcome and presented a performance award for 2010 to Judy Petsch, the forum's facilitator. He indicated he would highlight the WikiLeaks issue as part of the Computer Security Situational Awareness update.

Computer Security Policy, Standards, and Training Update

The following new standards, processes and templates were identified for the forum:

- New standards issued:
 - CSO-STD-0024, Organization Defined Values for System Security Assessment and Authorization Security Controls
 - CSO-STD-0026, Organization Defined Values for System Contingency Planning Security Controls
 - CSO-STD-5D01, Desktop Virtual Environment Configuration Standard
- New processes issued:
 - CSO-PROS-1314, NRC Web 2.0 Implementation Authorization Process
- New templates issued:
 - CSO-TEMP-1001, Request for Approval to Operate an External Web 2.0 Application
 - CSO-TEMP-1601, Enrollment Request for Computer Security Office (CSO) Provided Commercial IT Courses (Nationwide IT Services/Global Knowledge)

Awareness and Training

The bi-annual meeting for all (office and system) ISSOs occurred with a small gathering of attendees November 23, 8:30am-12:30pm in the auditorium. The forum was again reminded of the upcoming DHS Federal Virtual Training Environment and Federal Cybersecurity Training Exercise (Fed VTE/FedCTE) program. As information on its timeframe becomes available, more will be provided to the forum.

A reminder was given of the role-based training courses available to fulfill the FY11 requirement. Registration is required via iLearn. The spreadsheet that provides training requirements by office/personnel is available on CSO Training webpage <http://www.internal.nrc.gov/CSO/training.htm#FY11TrngRqmts>.

- Courses Availability
 - CSO sponsored role-based training courses availability
 - ISSO Role-based training course
 - April 26-28, 2011
 - Senior Level Manager/Executive Role-based training course
 - May 3, 2011, 1-3:00pm, room T8-A01
 - IT Manager/System Owner Role-based training course
 - May 4, 2011, 12:30-4:30pm, room T8-A01
 - System Administrator
 - March 29-30, 2011
 - May 11-13, 2011
 - June 28-30, 2011
 - August 29-31, 2011

Two commercially provided role-based training opportunities were covered with instruction on how to register for them.

- CSO Provided Commercial IT Security Role-Based Training Course "Fundamentals of Network Security", February 22-25, 2011 requires registration with CSO. There are five (5) seats reserved for contractors, at a reduced cost which the contractor is

responsible for paying. Cutoff date for course registration is February 14, 2011. Seats are on a first-come, first-serve basis. Should there be more contractors interested than the allotted for, CSO will work with the vendor and the interested office to address this.

- CSO-TEMP-1601 "Request to Enroll in Commercial IT Security Role-based Training via Computer Security Office (CSO) Nationwide IT Services/Global Knowledge Provided Contract," provides a list of courses that each office may select from to meet their IT security role training requirements. As identified in template CSO-TEMP-1601, the individual requesting the CSO provided training must obtain approval from his or her office ISSO to ensure the course is appropriate for the individual's IT role. The request memo is to be completed by the office ISSO and sent to the CSO Senior IT Security Officer for Policy, Standards, and Training. As identified in the template, there are Global Knowledge training centers located nearby the NRC headquarters and regional offices. Other locations are available but are dependent upon course offerings and will need to be coordinated with CSO and the vendor. Use of courses under this contract must occur before May 30, 2011 due to the expiration date of the contract.

The FY11 Annual Computer Security Awareness Course was added to everyone's iLearn Plan January 3, 2011. The due date for the course is August 15, 2011. There are new office completion metrics to be met quarterly and the bar chart on the CSO Training webpage was reset to zero as of January 3rd. CSO will run the quarterly reports for the offices at the end of each quarter and post the office completion percentages on the bar chart for easy reference.

Quarterly completion metrics:

- Q2 \geq 25%
- Q3 \geq 50%
- Q4 \geq 96%

NRC is partnering with the FAA for their 10th Annual FAA Information Technology/Information Systems Security (IT/ISS) Partnership and Training Conference, which will take place in Orlando, Florida March 14–18, 2011. CSO is providing two (2) courses, the Senior Manager/Executive Role-based course and the Computer Security for Overseas Travel with IT Assets. There is no registration cost to attend but travel must be covered by the individual's office. Attendance and participation in the training offered at the FAA IT/ISS Partnership and Training Conference (general sessions, information sessions, and workshops) satisfies the FISMA specialized training requirement. CSO is pursuing registration setup for NRC personnel.

FISMA Compliance and Oversight Team (FCOT) Update

XACTA implementation is ongoing with POA&M input scheduled to be completed by third quarter. CSO/FCOT is still looking for volunteers for this and is currently reviewing the functionality to make sure all information will be available. Training on the use of XACTA will occur. Individual systems will have one-on-one training to be more beneficial as the office's own data is entered. Each office will be scheduled. There is no anticipated additional cost for use of XACTA for each office. XACTA will allow for an office's Q&A documentation to be exportable to ADAMS since it's the official repository. The office will use the XACTA tool as the interface and won't need to recreate things. The XACTA tool and licenses have been purchased by CSO but the manpower resources to use the tool will be borne by the system owner.

Computer Security Situational Awareness (CSSA) Update

The Chair presented an overview, from a federal perspective, of the Wikileaks issue. Some of the documents that were leaked in December 2010 are considered National Security Information (classified). If someone were to pull up a website with this information, it would be considered an information spill as it would introduce classified information onto an unclassified computer system. To help protect the NRC network, access to the Wikileaks site has been blocked as well as to many other sites that have posted Wikileaks information. As a reminder to the forum, unless the information is formally declassified by the originating classifying authority (OCA), it remains classified. Release to the world does not constitute declassification. The need for information sharing in response to the terrorist threat has led to expanded access to classified information and may have eroded the application of the need-to-know (N-T-K) principle, which may have contributed to this type of leak. System owners and ISSOs need to review who has access to their system(s) to continually evaluate their N-T-K access. NSIR has been tasked as the lead office in responding to the OMB requirement for reviewing agency procedures with respect to security of classified information. NRC has until January 27, 2011 to respond. All offices should be prepared to respond to a request for assistance from NSIR to provide information needed for the NRC response. From an incident response view, NRC has to report any leaks that occur here. Additionally, access to the Wikileaks site is being externally monitored and as a federal employee, you should not access the site.

The Cyber Assessment Team Overview was provided to the forum. It is designated OUO-Security Related Information and will not be posted to the CSO website. The CAT has members from across the agency and a general understanding of what it does was provided to the forum.

The presentation for the Incident Response Database is OUO/Sensitive Security Information, so the brief will not be posted on the website. As general information, the forum was informed that various tools were assessed before a decision was made for the database tool. The CSO will assist and mature the process for use of this database to make better use of the data that is received. There is a granularity to the tool which will assist in better use by all stakeholders. Reporting capabilities will be available at all management levels. The tool will provide dashboards for ease of viewing.

ISSO Forum Decisions

None

Next Meeting:

February 8, 2010, 1:00-2:00pm, Room T-8-A01, bridge number: 886-390-1012; passcode:

(b)(6)