

From: Sand, Peter
To: Dean, Nicole M; Andrew, Emily; Brown, Michael A. RADM; Goode, Brendan; Rock, Lee
Cc: Eberle, Carole; Falkenstein, Cindy; Landesberg, Martha; (b) (6); (b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36; (b) (6)
Subject: RE: DPIAC/Cyber - Updated Agenda for 12/6 meeting
Date: Wednesday, November 16, 2011 8:30:05 AM
Attachments: Agenda 20111206 20111116.docx

Nicole,

Updated to add in DIB...

Good?

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6); pager: (b) (6)
(b) (6) www.dhs.gov/privacy

Join lively discussions with outside experts!
The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)
<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>
Reserve your spot in the front row! (b) (6)

From: Dean, Nicole M
Sent: Tuesday, November 15, 2011 3:42 PM
To: Sand, Peter; Andrew, Emily; Brown, Michael A. RADM; Goode, Brendan; Rock, Lee
Cc: Eberle, Carole; Falkenstein, Cindy; Landesberg, Martha; (b) (6); (b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Subject: RE: DPIAC/Cyber - Updated Agenda for 12/6 meeting

(b) (5)

From: Sand, Peter
Sent: Tuesday, November 15, 2011 1:27 PM
To: Andrew, Emily; Brown, Michael A. RADM; Dean, Nicole M; Goode, Brendan; Rock, Lee
Cc: Eberle, Carole; Falkenstein, Cindy; Landesberg, Martha; (b) (6); (b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Subject: DPIAC/Cyber - Updated Agenda for 12/6 meeting

All,

Attached please find an updated draft agenda for the next cyber subcommittee meeting.

Please feel free to edit at will!

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security

voice: (b) (6); pager: (b) (6)

(b) (6) www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6)

Andrew, Emily

From: Callahan, Mary Ellen (b) (6)
Sent: Thursday, April 07, 2011 11:08 AM
To: Sand, Peter; Callahan, Mary Ellen; PRIV Exec Sec
Cc: Kropf, John W; Andrew, Emily M
Subject: Re: [HEADS-UP] FW: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

Thanks. Agree (b) (5). Mec.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

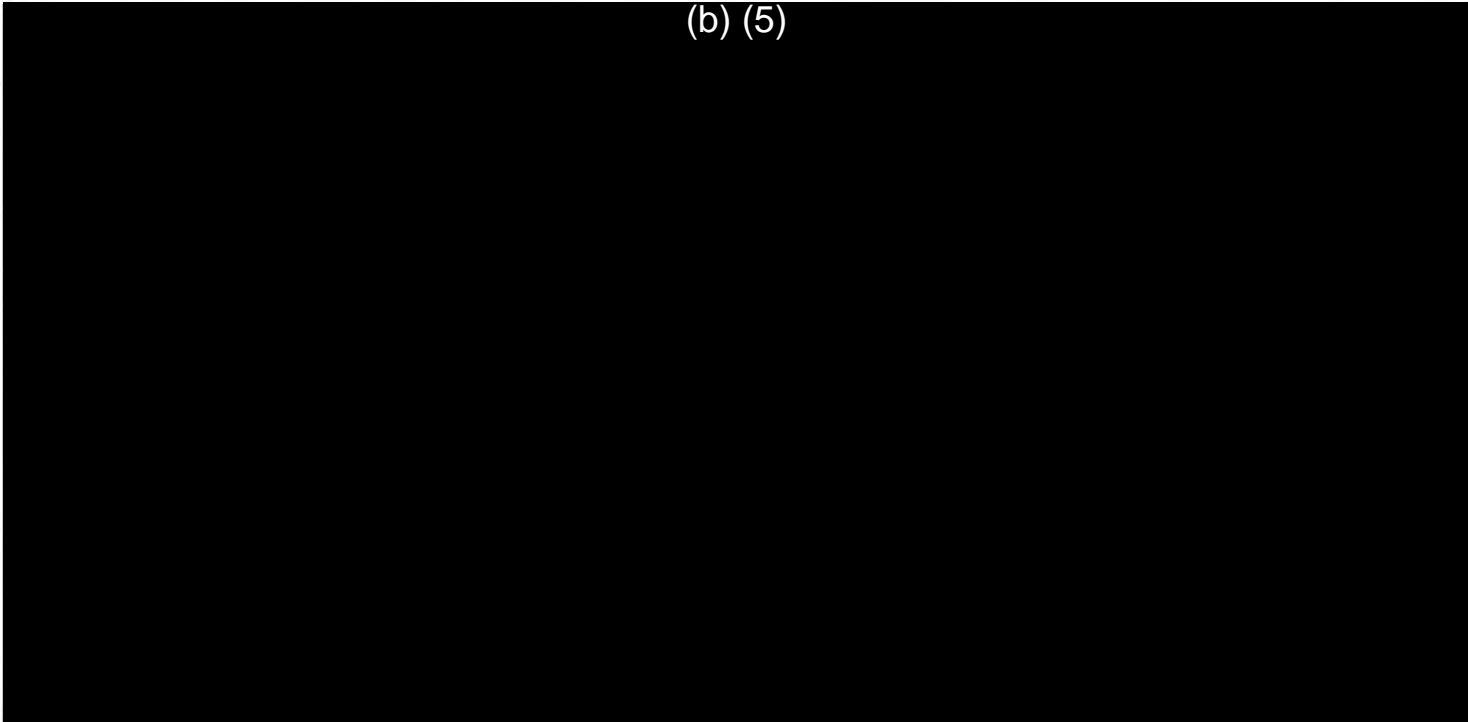
From: Sand, Peter (b) (6)
Sent: Thursday, April 07, 2011 11:00 AM
To: Callahan, Mary Ellen (b) (6); PRIV Exec Sec (b) (6)
Cc: Kropf, John (b) (6); Andrew, Emily M (b) (6)
Subject: RE: [HEADS-UP] FW: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

MEC,

I reviewed it and recommend clearing it with one comment: (b) (5)

In the main document, the paragraph (b) (5) - I suspect because other information in that paragraph is classified information.

(b) (5)



(b) (5)

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6) pager: (b) (6)
(b) (6) www.dhs.gov/privacy

From: PRIV Exec Sec (b) (6)
Sent: Wednesday, April 06, 2011 1:44 PM
To: Sand, Peter
Cc: Callahan, Mary Ellen; Kropf, John
Subject: [HEADS-UP] FW: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

Pete –

We will notify NPPD that you will be the POC for this tasker on Cybersecurity.

Thank you.

Sandy

Sandra L. Hawkins
Director of Administration
Privacy Office
U.S. Department of Homeland Security
245 Murray Lane, SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)
Fax: (b) (6)
E-mail: (b) (6)

This is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

From: (b) (6)
Sent: Wednesday, April 06, 2011 1:39 PM
To: (b) (6) (b) (6) Dorris, Earl; (b) (6) NPPDExecSec; NPPDtasking; (b) (6)
Cc: BriefingStaffA; Campbell, Sandra L; (b) (6) Plcy Exec Sec; (b) (6) OGC Exec Sec; (b) (6)
(b) (6) MGMTExecSec; (b) (6) (b) (6) (b) (6) I&A Exec Sec; CRCL

Exec Sec; PRIV Exec Sec; Privacy Office

Subject: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

The NSS is circulating a SECRET paper DC on cybersecurity and the DIB pilot asking for Deputy Secretary-level approval.

The documents were sent to Component Contacts on HSDN.

WHITE HOUSE ACTIONS TASKING

Document Name	NSS - Paper DC on Cybersecurity
Tracking Number	11.0005.73 / TBD
Lead Component	NPPD
Required Coordination	OGC, PLCY, MGMT, I&A, CRCL, PRIV
Product	<p><u>Requirement:</u></p> <ol style="list-style-type: none"> 1) Deputy Secretary-level comments/approval on the paper. Any edits or comments must be at the department-level and represent the One-DHS view. 2) Action Memo from NPPD Leadership to S2 recommending approval and transmittal of DHS response to the White House. 3) Completed Coordination Sheet detailing names of people from Components that have coordinated. (**We must receive this in order to consider the tasker complete**)
Notes	<p>COORDINATING COMPONENTS: Please work with NPPD as soon as possible.</p> <p>NPPD will lead and submit the final document to DHS Exec Sec.</p> <p><u>OGC Coordination:</u> Please ensure that briefing materials have been fully coordinated with OGC staff working in your component.</p> <p>If you anticipate being late with your comments please alert Lead Component and BriefingStaffA.</p>
Due	Thursday, April 7, 2011 (1700)

*Components listed in the "Required Coordination" shall provide a POC on this issue to NPPD as soon as possible upon receipt of this tasking.

Coordinating components should send unclassified responses/comments to NPPD and (b) (6)

NPPD should forward final consolidated response to ESEC.

(b) (6)

Office of the Executive Secretary
Office of the Secretary
Department of Homeland Security

(b) (6)

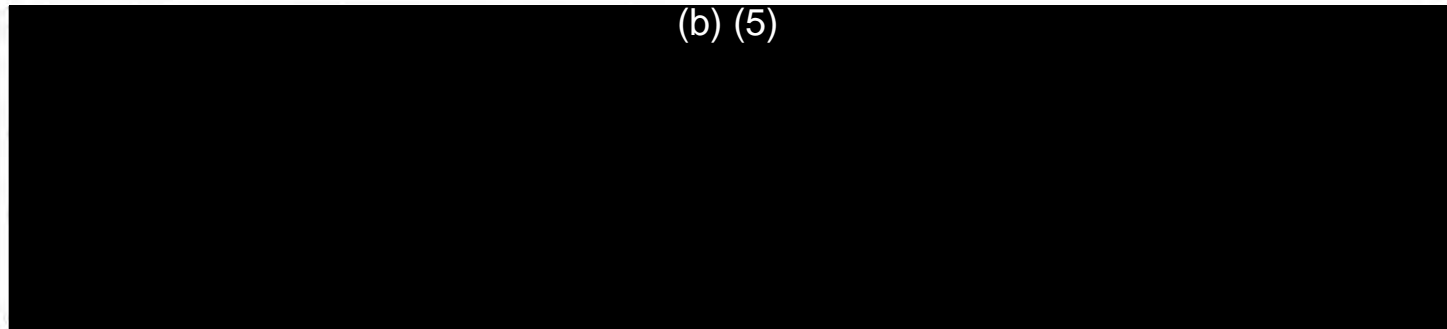
Andrew, Emily

From: Sand, Peter
Sent: Thursday, April 07, 2011 11:34 AM
To: PRIV Exec Sec
Cc: Andrew, Emily
Subject: RE: [HEADS-UP] FW: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

PRIV Exec Sec,

Please respond: PRIV clears with one comment:

(b) (5)



Thanks,

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6) pager: (b) (6)
(b) (6) www.dhs.gov/privacy

From: PRIV Exec Sec (b) (6)
Sent: Wednesday, April 06, 2011 1:44 PM
To: Sand, Peter
Cc: Callahan, Mary Ellen; Kropf, John
Subject: [HEADS-UP] FW: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

Pete –

We will notify NPPD that you will be the POC for this tasker on Cybersecurity.

Thank you.

Sandy

Sandra L. Hawkins
Director of Administration

Privacy Office
 U.S. Department of Homeland Security
 245 Murray Lane, SW, Mail Stop 0655
 Washington, DC 20528-0655
 Telephone: (b) (6)
 Fax: (b) (6)
 E-mail: (b) (6)

This is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

From: (b) (6)
Sent: Wednesday, April 06, 2011 1:39 PM
To: (b) (6); (b) (6); Dorris, Earl; (b) (6); NPPDExecSec; NPPDtasking; (b) (6)
Cc: BriefingStaffA; Campbell, Sandra L; (b) (6); Plcy Exec Sec; (b) (6); OGC Exec Sec; (b) (6); (b) (6); MGMTExecSec; (b) (6); (b) (6); (b) (6); I&A Exec Sec; CRCL Exec Sec; PRIV Exec Sec; Privacy Office
Subject: WHITE HOUSE ACTIONS TASKING - NSS - Paper DC on Cybersecurity - (Due 04.07.11, 1700)

The NSS is circulating a SECRET paper DC on cybersecurity and the DIB pilot asking for Deputy Secretary-level approval.

The documents were sent to Component Contacts on HSDN.

WHITE HOUSE ACTIONS TASKING

Document Name	NSS - Paper DC on Cybersecurity
Tracking Number	11.0005.73 / TBD
Lead Component	NPPD
Required Coordination	OGC, PLCY, MGMT, I&A, CRCL, PRIV
Product	<u>Requirement:</u> <ol style="list-style-type: none"> 1) Deputy Secretary-level comments/approval on the paper. Any edits or comments must be at the department-level and represent the One-DHS view. 2) Action Memo from NPPD Leadership to S2 recommending approval and transmittal of DHS response to the White House. 3) Completed Coordination Sheet detailing names of people from Components that have coordinated. (**We must receive this in order to consider the tasker complete**)

Notes	COORDINATING COMPONENTS: Please work with NPPD as soon as possible. NPPD will lead and submit the final document to DHS Exec Sec. <u>OGC Coordination:</u> Please ensure that briefing materials have been fully coordinated with OGC staff working in your component. If you anticipate being late with your comments please alert Lead Component and BriefingStaffA.
Due	Thursday, April 7, 2011 (1700)

*Components listed in the "Required Coordination" shall provide a POC on this issue to NPPD as soon as possible upon receipt of this tasking.

Coordinating components should send unclassified responses/comments to NPPD and (b) (6)

NPPD should forward final consolidated response to ESEC.

(b) (6)
Office of the Executive Secretary
Office of the Secretary
Department of Homeland Security
(b) (6)



Andrew, Emily

From: Parkinson, Deborah
Sent: Monday, November 28, 2011 10:14 AM
To: Andrew, Emily
Subject: Fw: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)
Attachments: 11.10.11 - NSS - Paper DC on DIB Pilot - SOC - 11.0005.188.pdf

From: Parkinson, Deborah
Sent: Tuesday, November 15, 2011 05:20 PM
To: McDermott, Thomas M
Subject: FW: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)

Deborah Parkinson
Deputy Chief of Staff
National Protection and Programs Directorate
Department of Homeland Security
office: (b) (6)
cell: (b) (6)

From: NPPDtasking
Sent: Tuesday, November 15, 2011 3:59 PM
To: CS&C EXEC SEC
Cc: Parkinson, Deborah; McConnell, Bruce; NPPDtasking; (b) (6) (b) (6)
Subject: FW: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)

CS&C,

For your awareness, please see attached for the Summary of Conclusions (SOC) from last week's Paper DC on DIB Pilot Extension. You'll note that there are follow-up actions outlined that are to be completed by DHS. Please share this information with your leadership.

V/r,
(b) (6)

(b) (6)
NPPD Exec Sec
Office: (b) (6)
BlackBerry: (b) (6)

From: (b) (6)
Sent: Tuesday, November 15, 2011 2:38 PM
To: (b) (6) (b) (6) Moore, Deborah O; NPPDExecSec; NPPDtasking; (b) (6)
Cc: BriefingStaffA; (b) (6) OGC Exec Sec; (b) (6) (b) (6) Campbell, Sandra L; Plcy Exec Sec; (b) (6) I&A Exec Sec; (b) (6) (b) (6) (b) (6) MGMTExecSec; (b) (6)
Subject: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)

Attached is the SOC from the Paper DC on DIB Pilot Extension. NPPD please note there are numerous actions for DHS.

From: (b) (6)
Sent: Wednesday, November 09, 2011 11:17 AM
To: (b) (6); (b) (6) Moore, Deborah O; NPPDExecSec; NPPDtasking; (b) (6)
Cc: BriefingStaffA; (b) (6) OGC Exec Sec; (b) (6); (b) (6) Campbell, Sandra L; Plcy Exec Sec;
 (b) (6) I&A Exec Sec; (b) (6); (b) (6); (b) (6); (b) (6); (b) (6)
 MGMTExecSec; Micone, Vincent; (b) (6) Williams, Derrick
Subject: White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)
Importance: High

The NSS is circulating a Paper DC on the DIB Pilot Extension for Deputy Secretary-level comment and approval.

WHITE HOUSE ACTIONS TASKING

Document Name	NSS - Paper DC on DIB Pilot Extension
Tracking Number	11.0005.188 / tbd
Lead Component	NPPD
Required Coordination	OGC, PLCY, I&A, MGMT
Product	<p><u>Requirement:</u></p> <ol style="list-style-type: none"> 1) Deputy Secretary-level comments/approval on the paper in a <i>consolidated</i> and <i>adjudicated</i> comment matrix. (**Matrix <u>must</u> speak in 1 unified DHS voice**) 2.) Action Memo from NPPD leadership to S2 recommending approval and transmittal of DHS response to the White House. 3) Completed Coordination Sheet detailing names of people from Components that have coordinated. (**We must receive this in order to consider the tasker complete**)
Notes	<p>COORDINATING COMPONENTS: Please work with NPPD as soon as possible.</p> <p>NPPD will lead and submit the final document to DHS Exec Sec.</p> <p><u>OGC Coordination:</u> Please ensure that briefing materials have been fully coordinated with OGC staff working in your component.</p> <p>If you anticipate being late with your comments please alert Lead Component and BriefingStaffA.</p>
Due	Thursday, November 10, 2011 (0900)

*Components listed in the "Required Coordination" shall provide a POC on this issue to NPPD as soon as possible upon receipt of this tasking.

Coordinating components should send unclassified responses/comments to NPPD and (b) (6)

NPPD should forward final consolidated response to ESEC.

(b) (6)

00011

Office of the Executive Secretary
Office of the Secretary
Department of Homeland Security

(b) (6)

Andrew, Emily

From: Goode, Brendan
Sent: Monday, December 19, 2011 5:30 PM
To: (b) (6) DISL OSD POLICY
Cc: Andrew, Emily; Falkenstein, Cindy V
Subject: Privacy inputs to NSS
Attachments: Privacy Oversight DHS task_20111219.docx

Hi (b) (6)

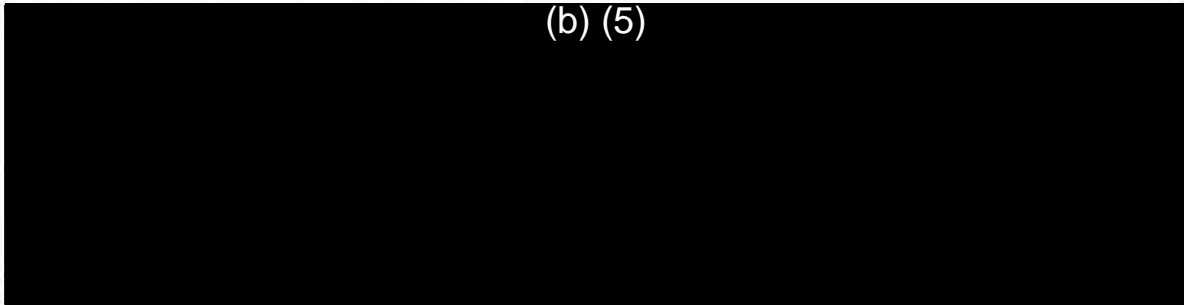
Attached is a draft of what we plan on submitting to NSS. I believe Emily (NPPD Privacy office) is getting final comments. We wanted to provide you situational awareness of our submission to NSS. How are you coming from your side?

Thanks,
Brendan

From: [Goode, Brendan](#)
To: [Dean, Nicole M](#); [McDermott, Thomas M](#); (b) (6); [Rock, Lee](#); [Harris, Richard](#); [Menna, Jenny](#); [Kizzee, Carlos](#); [Coose, Matt](#); [Smith, Mike C](#); [Donelan, Sean](#); [Delaney, Laura](#); (b) (6); (b) (6); (b) (6); [Jacobs, Michael](#); [Arnold, Patrick](#); [Allen, Brian](#); [Andrew, Emily](#); [Falkenstein, Cindy](#); [Fowler, Marita](#); (b)(3)-P.L. 86-36; (b) (6) "DISL OSD POLICY"
Subject: RE: JCSP Transition Activities
Date: Tuesday, December 20, 2011 4:31:38 PM

All-

For this evening's call, the agenda is:



(b) (5)

- Any open issues

We will attempt to keep the call brief, as I am sure most are trying to wrap up last minute items this week!

Brendan

-----Original Appointment-----

From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Tuesday, December 06, 2011 4:31 PM
To: Dean, Nicole M; McDermott, Thomas M; (b) (6) Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6) (b) (6); (b) (6); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Andrew, Emily; Falkenstein, Cindy; Fowler, Marita; (b)(3)-P.L. 86-36'; (b) (6) 'DISL OSD POLICY'
Subject: JCSP Transition Activities
When: Tuesday, December 27, 2011 5:00 PM-6:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: Phoncon 202-243-6160 #267946 (25 lines)

***UPDATED* as of 6 Dec 2011: 25 lines**

Dear (b) (6),

We are pleased to inform you that your reported Service Request has been resolved.

Reference No.: INC000000610090

Summary: Audio Bridge Correction - (b) (6) - Increase to 25 total lines.

Your reported Service Request has been resolved with the following resolution:

From: (b) (6)

Sent: Tuesday, December 06, 2011 3:26 PM

To: (b) (6)

Cc: CRMD ITSD Bridge Team

Subject: Audio Bridge Correction - Completed for INC000000610090

V/r,

(b) (6)

To ensure that we have the available ports for your conference please send in request at least 24 hours in advance. This will allow us to escalate the ticket in a timely fashion in the case that we don't have the available ports. We will still try our best to schedule your conference but this will increase the chances of availability.

Please dial into your conference at the appointed time. If you dial in before the time appointed you will not be able to enter the conference.

Dear Customer,

Please create a reminder on your calendar to renew 2 weeks prior to the ending date below to ensure that you get the same PIN number.

Your Conference bridge call has been confirmed, here is your DDI and Conference Pin number to access your conference. Please provide all participants in the conference with the DDI, and Conference Pin number.

DDI number: (b) (6) or (b) (6)

Conference Pin (b) (6)

Recurring Bridge Start Date/End Date: 11/28 – 12/29 2011

Ticket #: INC000000603227

Contact Name: (b) (6)

Email Address: (b) (6)

Contact Number: (b) (6)

Department: NPPD/CS&C

Justification/Existing PIN:

(Justification is REQUIRED for bridge lasting over 2 hours.)

Conference Call Date and time to be scheduled: 11/28 1700-1800

How Many Expected Participants: 20

Secure: NO

Classification: Unclassified

Recurring conference call: yes

If recurring is YES, enter: M-F through 2/29/2012

***If you have any complications with this bridge please call the following numbers immediately for adjustments or issues. ***

(b) (6) press 1 and ask for (b) (6)

From: [Andrew, Emily](#)
To: [McDermott, Thomas M](#); (b) (6); (b) (6); (b) (6); [Goode, Brendan](#); [Rock, Lee](#); [Brown, David](#); [Steiner, Kurt](#); [Jacobs, Michael](#)
Cc: [Falkenstein, Cindy](#); (b) (6); (b) (6)
Subject: Re: Draft NPPD JCSP PIA 20120110
Date: Tuesday, January 10, 2012 4:32:11 PM

(b) (5)

From: McDermott, Thomas M
Sent: Tuesday, January 10, 2012 02:24 PM
To: (b) (6); (b) (6); (b) (6); Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6); Andrew, Emily
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Tuesday, January 10, 2012 2:19 PM
To: (b) (6); (b) (6); McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6); Andrew, Emily
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

(b) (5)

(b) (6)

Attorney Advisor (Cybersecurity), DHS OGC

w: (b) (6)

m: (b) (6)

From: (b) (6)

Sent: Tuesday, January 10, 2012 1:56 PM

To: (b) (6) McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael; (b) (6)

Cc: Falkenstein, Cindy; (b) (6)

Subject: RE: Draft NPPD JCSP PIA 20120110

All,

For your reference. I'm attaching a redlined version which compares the document submitted to NPPD Privacy on Friday with the version that we received this morning. That might help with the review a bit.

(b) (6)

(b) (6)
DHS/NCSD/NSD

(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) (BlackBerry)

From: (b) (6)

Sent: Tuesday, January 10, 2012 10:59 AM

To: (b) (6) McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael; (b) (6)

Cc: Falkenstein, Cindy; (b) (6)

Subject: Fw: Draft NPPD JCSP PIA 20120110

Importance: High

All,

Attached is the latest version of the JCSP PIA. There are areas that require input from NSD, US-CERT, and OGC.

Please review and provide your edits to me by COB today so that I can consolidate all comments and get this back to Privacy by tomorrow's 12pm deadline (the thursday deadline below was a typo).

If you have any questions, please let me know.

Thanks,
Carolyn

From: Falkenstein, Cindy
Sent: Tuesday, January 10, 2012 10:49 AM
To: (b) (6)
Cc: McDermott, Thomas M; Goode, Brendan; (b) (6) Andrew, Emily
Subject: Draft NPPD JCSP PIA 20120110

Carolyn,
NPPD Privacy and DHS HQ Privacy have provided additional input; reviewed with comments that require input from NSD, OGC, and US-CERT. We have gone ahead and accepted most of the internal discussions, so this is a cleaned up version for an easier read and to help expedite the turn-around.

We have prepared MEC for a final draft by Friday and would like to have this back with your responses, ideally first thing in the AM, but by noon-Thursday, at the latest.

Thank you for all of your assistance in pulling this together.
Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: [Sand, Peter](#)
To: [McDermott, Thomas M](#); [Andrew, Emily](#); [Brosnihan, Carolyn](#)
Cc: (b) (6); [Richards, Rebecca](#); [Falkenstein, Cindy](#)
Subject: RE: Draft NPPD JCSP PIA 20120110
Date: Wednesday, January 11, 2012 12:49:11 PM

(b) (5)

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6) pager: (b) (6)
(b) (6) www.dhs.gov/privacy

Join lively discussions with outside experts!
The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)
<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>
Reserve your spot in the front row! (b) (6).

From: McDermott, Thomas M
Sent: Wednesday, January 11, 2012 12:21 PM
To: Andrew, Emily; (b) (6)
Cc: (b) (6); Richards, Rebecca; Falkenstein, Cindy; Sand, Peter
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Andrew, Emily
Sent: Wednesday, January 11, 2012 12:16 PM
To: McDermott, Thomas M; (b) (6)

Cc: (b) (6) Richards, Rebecca; Falkenstein, Cindy; Sand, Peter
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

Emily

From: McDermott, Thomas M
Sent: Wednesday, January 11, 2012 11:59 AM
To: Andrew, Emily; (b) (6) Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Andrew, Emily
Sent: Wednesday, January 11, 2012 11:55 AM
To: (b) (6) McDermott, Thomas M; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

Emily

From: (b) (6)
Sent: Wednesday, January 11, 2012 11:29 AM
To: McDermott, Thomas M; Falkenstein, Cindy; Andrew, Emily
Cc: (b) (6)
Subject: RE: Draft NPPD JCSP PIA 20120110

Thanks Tom. I'll incorporate this into our master consolidated comments document so that PRIV

just has to review one document with the revisions/responses.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: McDermott, Thomas M
Sent: Wednesday, January 11, 2012 11:27 AM
To: (b) (6) Falkenstein, Cindy; Andrew, Emily
Cc: (b) (6)
Subject: FW: Draft NPPD JCSP PIA 20120110
Importance: High

Attached are my comments on the PIA. (b) (5) (b) (5)

(b) (5)

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Wednesday, January 11, 2012 10:42 AM
To: McDermott, Thomas M; (b) (6)
Subject: RE: Draft NPPD JCSP PIA 20120110
Importance: High

Tom/(b) (6)

Do you have any other revisions/comments to the draft? I've got a little over an hour to get the next draft back to Privacy.

Thanks,
Carolyn

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: McDermott, Thomas M
Sent: Tuesday, January 10, 2012 2:24 PM
To: (b) (6) (b) (6) (b) (6) Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Andrew, Emily
Subject: RE: Draft NPPD JCSP PIA 20120110

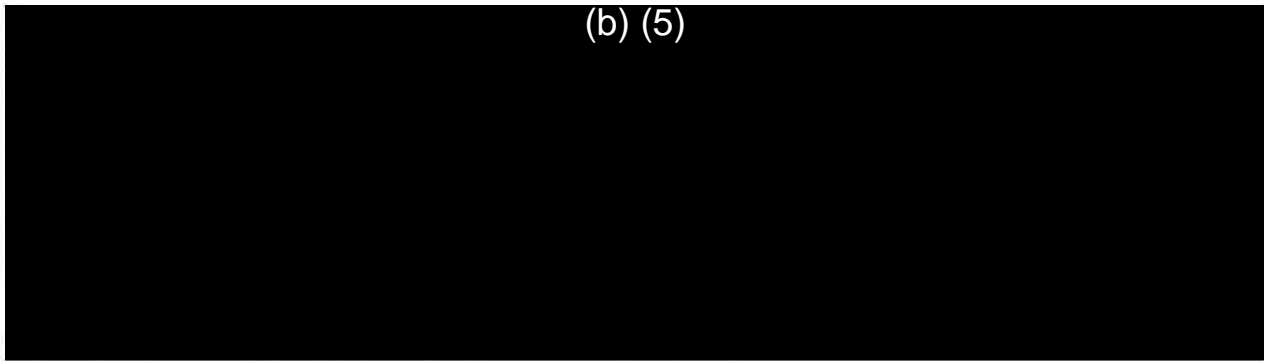
(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Tuesday, January 10, 2012 2:19 PM
To: (b) (6) (b) (6) McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Andrew, Emily
Subject: RE: Draft NPPD JCSP PIA 20120110

(b) (5)

(b) (5)



(b) (6)

Attorney Advisor (Cybersecurity), DHS OGC

w: (b) (6)

m: (b) (6)

From: (b) (6)

Sent: Tuesday, January 10, 2012 1:56 PM

To: (b) (6) McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael; (b) (6)

Cc: Falkenstein, Cindy; (b) (6)

Subject: RE: Draft NPPD JCSP PIA 20120110

All,

For your reference. I'm attaching a redlined version which compares the document submitted to NPPD Privacy on Friday with the version that we received this morning. That might help with the review a bit.

(b) (6)

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) 4 (BlackBerry)

From: (b) (6)

Sent: Tuesday, January 10, 2012 10:59 AM

To: (b) (6) McDermott, Thomas M; Goode, Brendan; Rock, Lee; Brown, David; Steiner, Kurt; Jacobs, Michael; (b) (6)

Cc: Falkenstein, Cindy; (b) (6)

Subject: Fw: Draft NPPD JCSP PIA 20120110

Importance: High

All,

Attached is the latest version of the JCSP PIA. There are areas that require input from NSD, US-CERT, and OGC.

Please review and provide your edits to me by COB today so that I can consolidate all comments and get this back to Privacy by tomorrow's 12pm deadline (the thursday deadline below was a typo).

If you have any questions, please let me know.

Thanks,

(b) (6)

From: Falkenstein, Cindy
Sent: Tuesday, January 10, 2012 10:49 AM
To: (b) (6)
Cc: McDermott, Thomas M; Goode, Brendan; (b) (6) Andrew, Emily
Subject: Draft NPPD JCSP PIA 20120110

(b) (6)

NPPD Privacy and DHS HQ Privacy have provided additional input; reviewed with comments that require input from NSD, OGC, and US-CERT. We have gone ahead and accepted most of the internal discussions, so this is a cleaned up version for an easier read and to help expedite the turn-around.

We have prepared MEC for a final draft by Friday and would like to have this back with your responses, ideally first thing in the AM, but by noon-Thursday, at the latest.

Thank you for all of your assistance in pulling this together.

Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: Falkenstein, Cindy
To: Sand, Peter; Andrew, Emily; Rebecca J. Richards [REDACTED] (b) (6)
Cc: Lockett, Vania
Subject: RE: JCSP DRAFT PIA -
Date: Thursday, January 12, 2012 10:28:33 AM

Pete,
I've verified that you have all the same edits that [REDACTED] (b) (6) sent over this AM, so once accepted, your formatted doc. should be good to go.
Thanks,
Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. [REDACTED] (b) (6) | Arlington VA 22201 | ☎ [REDACTED] (b) (6) (O) | ✉ [REDACTED] (b) (6) (BB) |
✉ [REDACTED] (b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: Sand, Peter
Sent: Thursday, January 12, 2012 10:21 AM
To: Falkenstein, Cindy; Andrew, Emily; Rebecca J. Richards [REDACTED] (b) (6)
Cc: Lockett, Vania
Subject: RE: JCSP DRAFT PIA -

Cindy, Emily,

I made the changes in the version I cleaned up from last night (to avoid reformatting new document again). [REDACTED] (b) (5)
[REDACTED] (b) (5)

Since we're bouncing between different documents, could you confirm that I am making the same edits in the version that just came back from the program office? - see redlines.

Once I hear back from you, I will create a clean version and then I guess we wait to see if anything comes back from DOD/NSA... still don't know about NSS.

Then it'll be ready for MEC's review - right, Becky?

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: [REDACTED] (b) (6) pager: [REDACTED] (b) (6)
[REDACTED] (b) (6) www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6)

From: Falkenstein, Cindy
Sent: Thursday, January 12, 2012 10:05 AM
To: Andrew, Emily; Sand, Peter
Cc: Lockett, Vania
Subject: RE: JCSP DRAFT PIA -

I've reviewed, and cleaned, but am sending two copies so you can reference. If the edits/comments are acceptable, which they seem to be to me, then the cleaned copy is the one to go forward on.

Shall we send to PIA? Or are we still waiting on the DOD and NSS responses?

Let me know.

Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | ☎ (b) (6) (O) | 📠 (b) (6) (BB) |
✉ (b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: Andrew, Emily
Sent: Thursday, January 12, 2012 10:02 AM
To: Sand, Peter; Falkenstein, Cindy
Subject: Fw: JCSP DRAFT PIA -
Importance: High

Pete and Cindy this is the version to review.

From: (b) (6)
Sent: Thursday, January 12, 2012 09:36 AM
To: Andrew, Emily; Richards, Rebecca; Sand, Peter; (b) (6) Rock, Lee; Goode, Brendan; McDermott, Thomas M
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6) Brown, David
Subject: RE: JCSP DRAFT PIA -

Emily --

Please find our revised version attached, (b) (5)
(b) (5).

Thanks,

(b) (6)

(b) (6)
DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily

Sent: Wednesday, January 11, 2012 4:27 PM

To: Richards, Rebecca; Sand, Peter; (b) (6) (b) (6) Rock, Lee; Goode, Brendan; McDermott, Thomas M

Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)

Subject: JCSP DRAFT PIA -

Importance: High

All,

Please find attached a clean version of the DRAFT JCSP PIA. There are a few outstanding areas that need to be reviewed and confirmed for accuracy. (b) (5)

(b) (5)

I've also included (b) (6) earlier version from today so that you could see all comments and changes.

US-CERT – we need your comments ASAP.

Becky – can you check with Mary Ellen on how she'd like the clean version disseminated to DOD and NSS? I think it's ready to go we just need to make sure that comments are received in time to adjudicate and have signed off by Friday.

Let me know if anyone has questions.

Emily

Emily Andrew, CIPP, CIPP/G | Sr. Privacy Officer
National Protection and Programs Directorate | U.S. Department of Homeland Security
1616 N. Ft. Myer Dr. (b) (6) | Arlington VA 22209 | (b) (6) | (b) (6)

From: [Andrew, Emily](#)
To: [Callahan, Mary Ellen](#); [Sand, Peter](#)
Cc: [Falkenstein, Cindy](#); ["Rebecca J. Richards"](#) (b) (6) PIA
Subject: RE: PIA NPPD NCPS (DHS DIB Pilot) - for your review
Date: Thursday, January 12, 2012 8:32:08 PM
Attachments: [DHS_PIA_NPPD_JCSP_Draft_20120111\(2\)_VM_DC3_edits-comments.doc](#)

Mec – thanks for reviewing. We did receive comments back from DoD late this evening (attached). The comments and/or suggested changes (b) (5) but many of the questions have to be answered by US-CERT. We have a call scheduled with them tomorrow at 1130.

Becky – since you'll have the hard copy – how should we coordinate the changes? I just got called to a 3 ½ hour meeting at the NAC (w/Rand) tomorrow morning but Cindy and (b) (6) are available to keep this morning. I believe (b) (6) is working some of the changes right now.

Emily

From: Callahan, Mary Ellen
Sent: Thursday, January 12, 2012 7:53 PM
To: Sand, Peter; Callahan, Mary Ellen
Cc: Andrew, Emily; Falkenstein, Cindy; Rebecca J. Richards (b) (6) PIA
Subject: RE: PIA NPPD NCPS (DHS DIB Pilot) - for your review

I edited it in hard copy, in my outbox. (b) (5)

. Mec

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)
Fax: (b) (6)
E-mail: (b) (6)
Website: www.dhs.gov/privacy

From: Sand, Peter
Sent: Thursday, January 12, 2012 2:29 PM
To: Callahan, Mary Ellen
Cc: Andrew, Emily; Falkenstein, Cindy; Rebecca J. Richards (b) (6) PIA
Subject: PIA NPPD NCPS (DHS DIB Pilot) - for your review

MEC,

Here's the current draft of the PIA – for your review. All PRIV/NPPD comments have been adjudicated.

We are waiting on any comments that might come from Michael E. Reheuser

(b) (6) or (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 - gave them both deadline for 8 a.m. tomorrow.

I put it in a green folder for your review and will update it/tell you about any comments we get back from Mike or John tomorrow morning.

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security

voice: (b) (6) pager: (b) (6)

(b) (6) www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6).

From: [Sand, Peter](#)
To: (b) (6)
Cc: [Andrew, Emily](#); [Falkenstein, Cindy](#)
Subject: Re: PIA NPPD NCPS (DHS DIB Pilot) - for your review
Date: Thursday, January 12, 2012 9:24:31 PM

Becky - if you could redline MEC's changes and email it to me, I can reconcile with what we do with DOD's stuff?

Pete

Peter E. Sand
DHS PRIV, (b) (6)
Sent via blackberry.
Please excuse the effects of big thumbs on little keys.

From: Callahan, Mary Ellen
Sent: Thursday, January 12, 2012 07:53 PM
To: Sand, Peter; Callahan, Mary Ellen
Cc: Andrew, Emily; Falkenstein, Cindy; Rebecca J. Richards (b) (6)
(b) (6) >; PIA
Subject: RE: PIA NPPD NCPS (DHS DIB Pilot) - for your review

I edited it in hard copy, in my outbox. (b) (5)

[REDACTED]
[REDACTED] Mec

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)
Fax: (b) (6)
E-mail: (b) (6)
Website: www.dhs.gov/privacy

From: Sand, Peter
Sent: Thursday, January 12, 2012 2:29 PM
To: Callahan, Mary Ellen
Cc: Andrew, Emily; Falkenstein, Cindy; Rebecca J. Richards (b) (6) PIA
Subject: PIA NPPD NCPS (DHS DIB Pilot) - for your review

MEC,

Here's the current draft of the PIA - for your review. All PRIV/NPPD comments have been adjudicated.

We are waiting on any comments that might come from Michael E. Reheuser
(b) (6) or (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 - gave them
both deadline for 8 a.m. tomorrow.

I put it in a green folder for your review and will update it/tell you
about any comments we get back from Mike or John tomorrow morning.

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6) pager: (b) (6)
(b) (6); www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series

(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6)

Andrew, Emily

From: Richards, Rebecca
Sent: Friday, January 13, 2012 2:32 PM
To: Sand, Peter; Andrew, Emily
Subject: FW: JCSP PIA - OSD Comments Adjudicated
Attachments: DHS_PIA NPPD JCSP Draft 20120111 (2)_VM +DC3 edits-comments +MEC_Adjudicated.doc; DHS_PIA NPPD JCSP Draft 20120111 (2)_VM +DC3 edits-comments +MEC_Adjudicated_no comments.doc

Importance: High

Pete:

When you are done with Admiral :) can you touch base with Emily on the responses back to DOD. We need to send those tonight. I am going forward with MEC signing.

Thanks,
Becky

Becky Richards
DHS Privacy Office
(b) (6)

From: (b) (6)
Sent: Friday, January 13, 2012 12:30 PM
To: Andrew, Emily
Cc: Falkenstein, Cindy; Goode, Brendan; (b) (6) McDermott, Thomas M; (b) (6) Brown, David; Steiner, Kurt; Richards, Rebecca; Sand, Peter
Subject: JCSP PIA - OSD Comments Adjudicated
Importance: High

Emily –

Attached is the adjudicated version of the PIA, which reflects the discussion from this morning’s call. There are two versions, one redlined to go to MEC and the second includes comment adjudications to go back to OSD, if needed.

Please let us know if there is anything else you need.

(b) (6)

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

Andrew, Emily

From: Andrew, Emily
Sent: Friday, January 13, 2012 5:02 PM
To: Richards, Rebecca; Sand, Peter
Subject: Re: JCSP PIA - OSD Comments Adjudicated

That is awesome news. Thank you both for your help on this. We will have the NCPS to Pete next week.

From: Richards, Rebecca
Sent: Friday, January 13, 2012 04:59 PM
To: Andrew, Emily; Sand, Peter
Subject: RE: JCSP PIA - OSD Comments Adjudicated

PIA is signed and being sent to web publishing right now. Will send PDF when it is done shortly.

Becky Richards
DHS Privacy Office
[REDACTED] (b) (6)

From: Andrew, Emily
Sent: Friday, January 13, 2012 4:58 PM
To: Sand, Peter; Richards, Rebecca
Subject: Re: JCSP PIA - OSD Comments Adjudicated

I'm getting on my evening call. I'll send you a message when I'm off.

From: Sand, Peter
Sent: Friday, January 13, 2012 04:12 PM
To: Richards, Rebecca; Andrew, Emily
Subject: Re: JCSP PIA - OSD Comments Adjudicated

Emily, I'm in the car too - will let you know when I get home to chat...

Becky - do we know when it will publish?

Pete

Peter E. Sand
DHS PRIV, [REDACTED] (b) (6)
Sent via blackberry.
Please excuse the effects of big thumbs on little keys.

From: Richards, Rebecca
Sent: Friday, January 13, 2012 04:11 PM
To: Sand, Peter; Andrew, Emily
Subject: RE: JCSP PIA - OSD Comments Adjudicated

It is with MEC – just want you to tell DOD we didn't take anything> Emily wanted to talk you through the responses. She is in the car now. [REDACTED] (b) (6)

00034

Becky Richards
DHS Privacy Office

(b) (6)

From: Sand, Peter
Sent: Friday, January 13, 2012 4:10 PM
To: Richards, Rebecca; Andrew, Emily
Subject: Re: JCSP PIA - OSD Comments Adjudicated

I just finished - have to drive home - is there anything left to do before sending to MEC?

Pete

Peter E. Sand
DHS PRIV, (b) (6)
Sent via blackberry.
Please excuse the effects of big thumbs on little keys.

From: Richards, Rebecca
Sent: Friday, January 13, 2012 02:32 PM
To: Sand, Peter; Andrew, Emily
Subject: FW: JCSP PIA - OSD Comments Adjudicated

Pete:

When you are done with Admiral :) can you touch base with Emily on the responses back to DOD. We need to send those tonight. I am going forward with MEC signing.

Thanks,
Becky

Becky Richards
DHS Privacy Office

(b) (6)

From: (b) (6)
Sent: Friday, January 13, 2012 12:30 PM
To: Andrew, Emily
Cc: Falkenstein, Cindy; Goode, Brendan; (b) (6) McDermott, Thomas M; (b) (6) Brown, David; Steiner, Kurt; Richards, Rebecca; Sand, Peter
Subject: JCSP PIA - OSD Comments Adjudicated
Importance: High

Emily –

Attached is the adjudicated version of the PIA, which reflects the discussion from this morning's call. There are two versions, one redlined to go to MEC and the second includes comment adjudications to go back to OSD, if needed.

Please let us know if there is anything else you need.

(b) (6)

00035

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

From: [Falkenstein, Cindy](#)
To: [Ward, Linda COS](#); [Stubbs, Lee](#)
Subject: FW: U.S. Department of Homeland Security Privacy Impact Assessments (PIA) Update
Date: Tuesday, January 17, 2012 3:09:00 PM

Linda and Lee,

I wanted to be sure you both were aware of the recent posting to the DHS website for a CS&C project. The Joint Cybersecurity Services Pilot (JCSP) PIA was signed on Friday and published today to the DHS website ([link below](#)). A lot of time and effort on behalf of CS&C went into making this publication possible.

Thank you,
 Cindy

Cindy Falkenstein
 Senior Privacy Analyst for Cyber Security & Communications (CS&C)
 Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
 1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
 (b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: Andrew, Emily
Sent: Tuesday, January 17, 2012 9:48 AM
To: (b) (6) Goode, Brendan; McDermott, Thomas M; Gillis, Ryan M; (b) (6)
Cc: Falkenstein, Cindy
Subject: FW: U.S. Department of Homeland Security Privacy Impact Assessments (PIA) Update

The PIA is officially posted on the DHS website.

From: U.S. Department of Homeland Security (b) (6)
Sent: Tuesday, January 17, 2012 9:34 AM
To: (b) (6)
Subject: U.S. Department of Homeland Security Privacy Impact Assessments (PIA) Update

You are subscribed to Privacy Impact Assessments (PIA) for U.S. Department of Homeland Security. This information has recently been updated.

PIA-021 - National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP)

DHS/NPPD/PIA-021 [National Cyber Security Division Joint Cybersecurity Services Pilot \(JCSP\)](#), January 13, 2012 (*PDF, 16 pages – 248 KB*). The Department of Homeland Security (DHS) and the Department of Defense (DoD) are jointly undertaking a proof of concept known as the Joint Cybersecurity Services Pilot (JCSP). The JCSP extends the existing operations of the Defense Industrial Base (DIB) Exploratory Cybersecurity Initiative (DIB Opt-In Pilot) and shifts the operational relationship with the CSPs in the pilot to DHS. The JCSP is part of overall efforts by DHS and DoD to enable the provision of cybersecurity capabilities enhanced by U.S. government information to protect critical infrastructure

information systems and networks. The purpose of the JCSP is to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect sensitive DoD information and DIB intellectual property that directly supports DoD missions or the development of DoD capabilities from unauthorized access, exfiltration, and exploitation. The National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) on behalf of DHS because some known or suspected cyber threat information shared under the JCSP may contain information that could be considered personally identifiable information (PII).

Associated SORN(s):

- DHS/ALL-002 - [Department of Homeland Security \(DHS\) Mailing and Other Lists System](#) November 25, 2008, 73 FR 71659



Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your e-mail address to log in. If you have questions or problems with the subscription service, please contact support@govdelivery.com.

This service is provided to you at no charge by the [U.S. Department of Homeland Security](#).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.



From: [Andrew, Emily](#)
To: (b) (6)
Cc: [Goode, Brendan](#); [McDermott, Thomas M](#); [Falkenstein, Cindy](#)
Subject: RE: Question re JCSP PIA
Date: Thursday, January 19, 2012 6:41:28 AM

(b) (6) – can you assist with responses from questions from CDT on the JCSP? (b) (5)
Once we have them reviewed by our team we can shoot them over to DoD to make sure they are okay with them as well.

Emily

The question is this:

(b) (5)

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)

was associated with the alert

3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

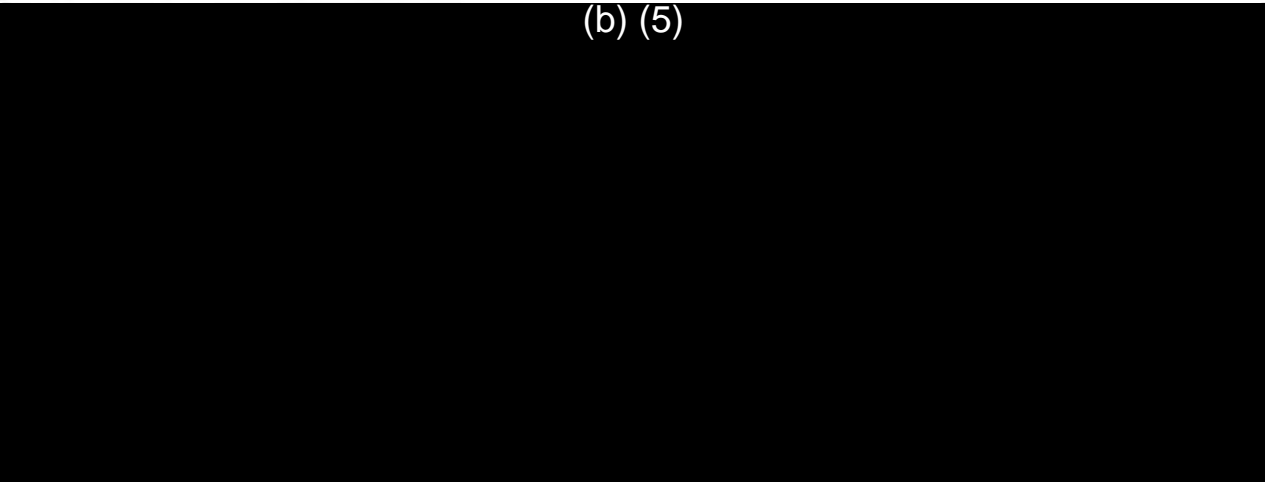
•

4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

From: Goode, Brendan
Sent: Wednesday, January 18, 2012 6:43 PM
To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(b) (5)



Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: Sand, Peter
Sent: Wednesday, January 18, 2012 3:03 PM
To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006
(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: [McDermott, Thomas M](#)
To: [Andrew, Emily](#); (b) (6)
Cc: [Goode, Brendan](#); [Falkenstein, Cindy](#)
Subject: RE: Question re JCSP PIA
Date: Thursday, January 19, 2012 9:04:54 AM

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 6:41 AM
To: (b) (6)
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

(b) (6) – can you assist with responses from questions from CDT on the JCSP? T (b) (5)
(b) (6) Once we have them reviewed by our team we can shoot them over to DoD to make sure they are okay with them as well.

Emily

(b) (5)

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files

Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)

3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

•

4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

From: Goode, Brendan

Sent: Wednesday, January 18, 2012 6:43 PM

To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha

Subject: RE: Question re JCSP PIA

(b) (5)

(b) (5)

Thanks,
Brendan

Office: (b) (6)
Blackberry: 202-203-9538

From: Sand, Peter
Sent: Wednesday, January 18, 2012 3:03 PM
To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the

question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

IP address

Domain

Email header

Files

Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006

(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: Sand, Peter
To: Andrew, Emily; (b) (6)
Cc: Falkenstein, Cindy
Subject: RE: Question re JCSP PIA
Date: Thursday, January 19, 2012 3:01:01 PM

Emily,

(b) (5)

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security

(b) (6) (b) (6)

www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 2:07 PM
To: (b) (6) Sand, Peter
Cc: Falkenstein, Cindy
Subject: FW: Question re JCSP PIA

Before I send to the rest of the group. See attached document and let me know what you think.

(b) (5)

From: McDermott, Thomas M
Sent: Thursday, January 19, 2012 9:28 AM
To: (b) (6) Andrew, Emily
Cc: Goode, Brendan; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs

desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Thursday, January 19, 2012 9:04 AM
To: Andrew, Emily
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

Proposed updates to 1, 2, and 3 are below. (b) (5)
(b) (5) The PII is only used if it's directly related to a
cyber threat (per US-CERT SOPs), so I'm not really sure what he's asking.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 6:41 AM
To: (b) (6)
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

(b) (6) – can you assist with responses from questions from CDT on the JCSP? (b) (5)
(b) (6) Once we have them
reviewed by our team we can shoot them over to DoD to make sure they are okay with them
as well.

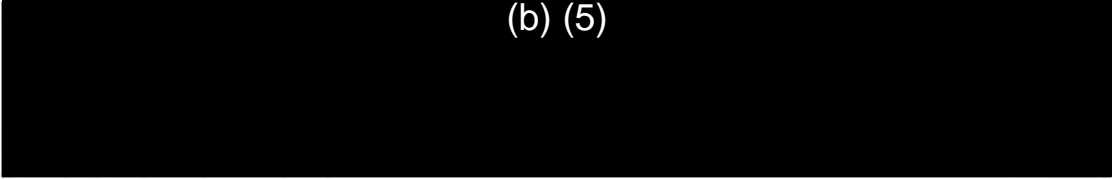
Emily

The question is this:

1. What information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

(b) (5)

(b) (5)



The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

IP address

Domain

Email header

Files

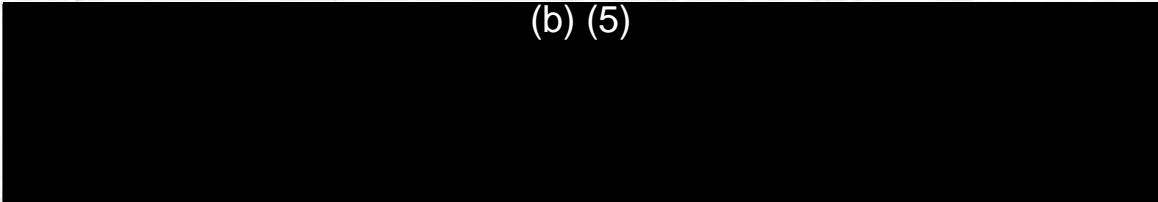
Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

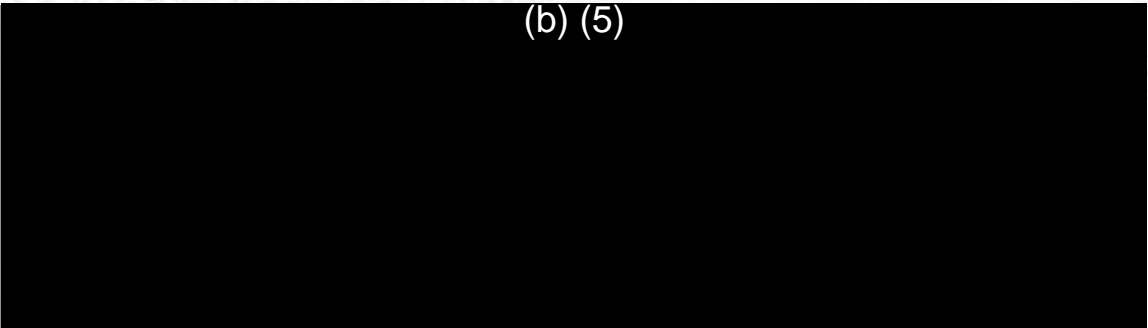
2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)



3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

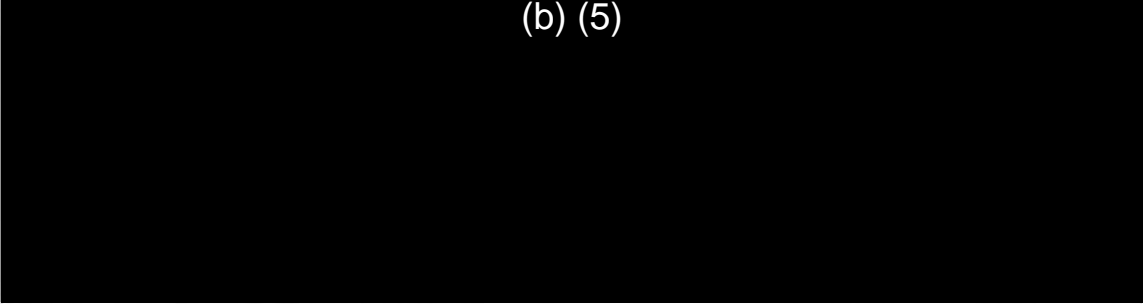
(b) (5)



4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header,

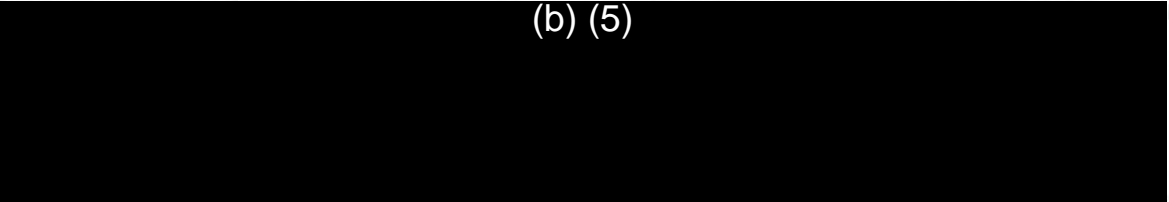
and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

(b) (5)



5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

(b) (5)



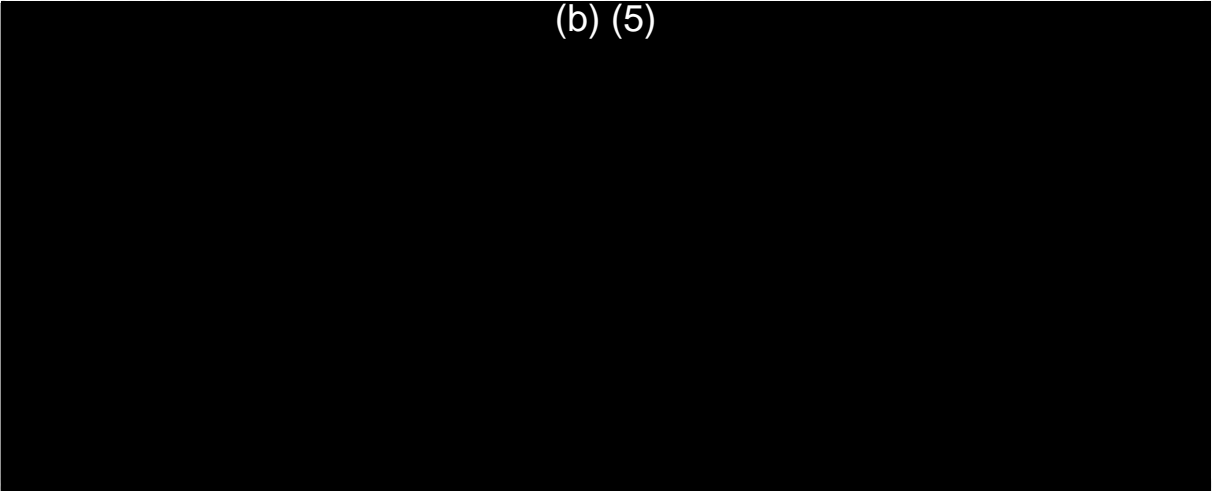
From: Goode, Brendan

Sent: Wednesday, January 18, 2012 6:43 PM

To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha

Subject: RE: Question re JCSP PIA

(b) (5)



Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: Sand, Peter

Sent: Wednesday, January 18, 2012 3:03 PM

To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006

(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: [Andrew, Emily](#)
To: [McDermott, Thomas M](#); [Goode, Brendan](#)
Cc: [Sand, Peter](#); [Falkenstein, Cindy](#)
Subject: FW: Question re JCSP PIA
Date: Friday, January 20, 2012 9:46:45 AM
Importance: High

Tom / Brendan – are you okay with the language below? And do you still think we need to send to DoD? If you are okay with it I'll have Mec forward on to Greg.

I'll be without my BB starting at 1030 until later this afternoon so I was hoping to wrap this up this morning.

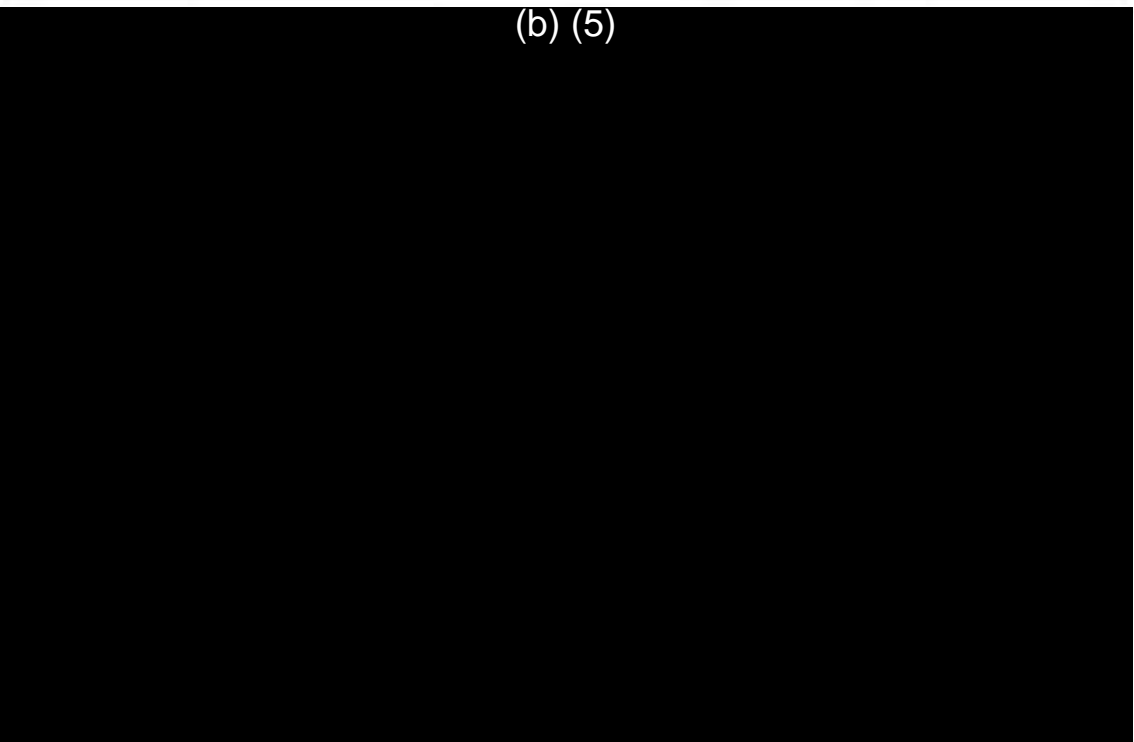
Thanks
Emily

From: Andrew, Emily
Sent: Thursday, January 19, 2012 3:56 PM
To: McDermott, Thomas M; Goode, Brendan; (b) (6)
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)
Subject: RE: Question re JCSP PIA

Here's the latest draft response. Let me know if you are okay with this version or have any further edits. (b) (5)

Emily

(b) (5)



From: McDermott, Thomas M
Sent: Thursday, January 19, 2012 9:28 AM
To: (b) (6) Andrew, Emily
Cc: Goode, Brendan; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

See comments below in red.

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Thursday, January 19, 2012 9:04 AM
To: Andrew, Emily
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

Proposed updates to 1, 2, and 3 are below. (b) (5)
(b) (5). The PII is only used if it's directly related to a
cyber threat (per US-CERT SOPs), so I'm not really sure what he's asking.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 6:41 AM
To: (b) (6)
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

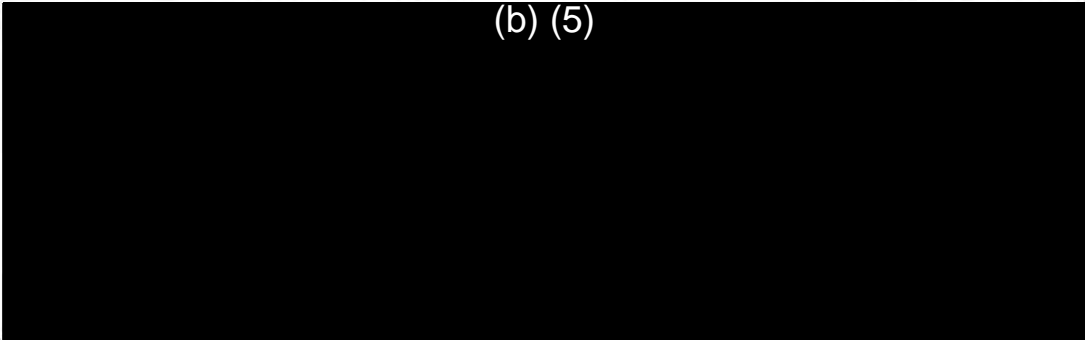
(b) (5)

Emily

The question is this:

1. What information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

(b) (5)



The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

IP address

Domain

Email header

Files

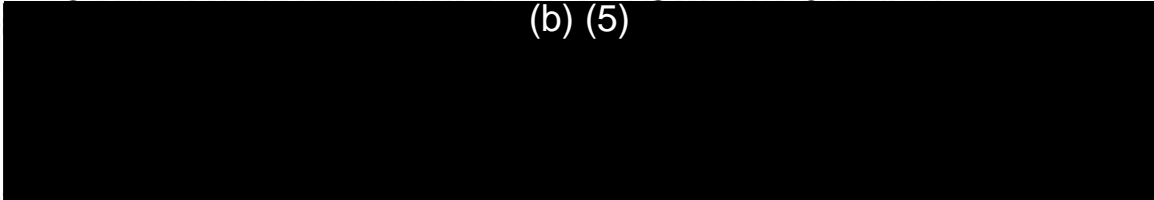
Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

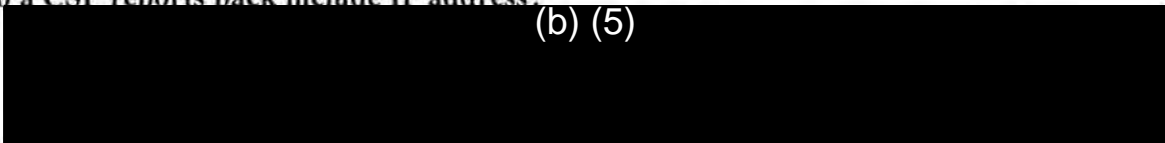
2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)



3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

(b) (5)



(b) (5)

4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

(b) (5)

5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

(b) (5)

From: Goode, Brendan

Sent: Wednesday, January 18, 2012 6:43 PM

To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha

Subject: RE: Question re JCSP PIA

(b) (5)

Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: Sand, Peter
Sent: Wednesday, January 18, 2012 3:03 PM
To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_icsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service

Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006
(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: (b) (6)
To: [Andrew, Emily](#); [McDermott, Thomas M](#); [Goode, Brendan](#); [Ritz, Daniel](#)
Cc: [Falkenstein, Cindy](#); [Sand, Peter](#)
Subject: RE: Question re JCSP PIA
Date: Friday, January 20, 2012 2:00:25 PM

Emily –

Brendan's feedback is below. Otherwise, he believes this is good to go.

(b) (6)

(b) (6)
DHS/NCSD/NSD

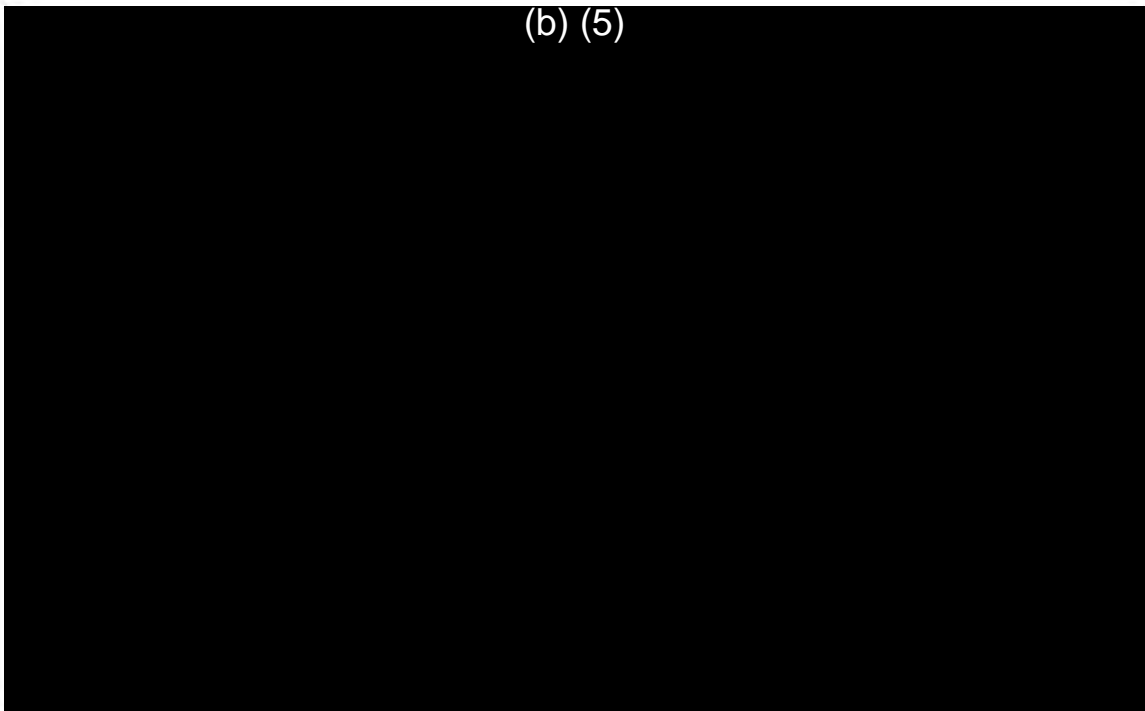
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 3:56 PM
To: McDermott, Thomas M; Goode, Brendan; (b) (6)
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)
Subject: RE: Question re JCSP PIA

Here's the latest draft response. Let me know if you are okay with this version or have any further edits. Also – since we kept this high level – let me know if we need to socialize with DoD and if so, who should we send it to.

Emily

(b) (5)



(b) (5)

From: McDermott, Thomas M
Sent: Thursday, January 19, 2012 9:28 AM
To: (b) (6) Andrew, Emily
Cc: Goode, Brendan; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Thursday, January 19, 2012 9:04 AM
To: Andrew, Emily
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

Proposed updates to 1, 2, and 3 are below. (b) (5)
(b) (5) The PII is only used if it's directly related to a
cyber threat (per US-CERT SOPs), so I'm not really sure what he's asking.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 6:41 AM
To: (b) (6)
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

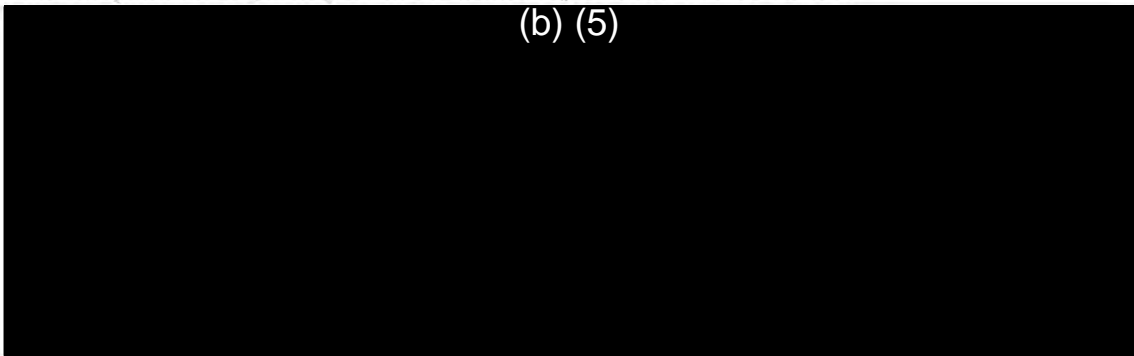
(b) (6) – can you assist with responses from questions from CDT on the JCSP? (b) (5)
(b) (6) Once we have them
reviewed by our team we can shoot them over to DoD to make sure they are okay with them
as well.

Emily

The question is this:

1. What information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

(b) (5)



The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

IP address

Domain

Email header

Files

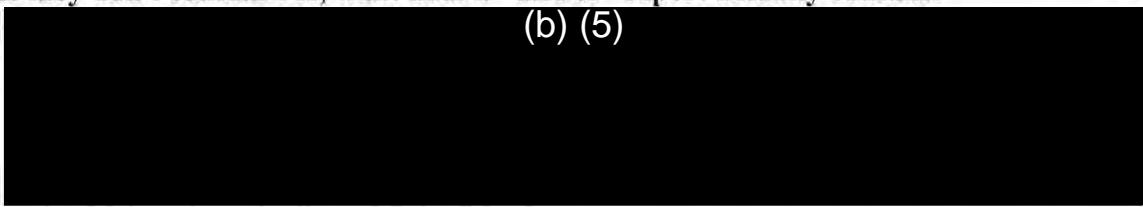
Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)



3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

(b) (5)



(b) (5)

4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

(b) (5)

5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

(b) (5)

From: Goode, Brendan

Sent: Wednesday, January 18, 2012 6:43 PM

To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha

Subject: RE: Question re JCSP PIA

(b) (5)

Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: Sand, Peter
Sent: Wednesday, January 18, 2012 3:03 PM
To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
 Senior Counsel and
 Director, Project on Freedom, Security & Technology
 Center for Democracy & Technology
 1634 Eye St., NW (b) (6)
 Washington, DC 20006
 (b) (6) direct
 (b) (6) fax
 (b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: [Andrew, Emily](#)
To: [Callahan, Mary Ellen](#)
Cc: [Sand, Peter](#); [Goode, Brendan](#); (b) (6) [McDermott, Thomas M](#); [Falkenstein, Cindy](#); [Landesberg, Martha](#)
Subject: RE: Question re JCSP PIA
Date: Friday, January 20, 2012 3:30:55 PM

Mary Ellen,

Below is the response to the questions on the JCSP PIA from Greg. The response has been reviewed and approved by NSD and OGC. (b) (5)

[Redacted]

Emily

(b) (5)

[Large Redacted Block]

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) [McDermott, Thomas M](#)
Subject: Fw: Question re JCSP PIA

(b) (5)

[Redacted]

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006
(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: [Callahan, Mary Ellen](#)
To: [Greg Nojeim](#); [Mary Ellen Callahan](#)
Subject: RE: Question re JCSP PIA
Date: Friday, January 20, 2012 4:03:08 PM

Hi Greg:

Thank you for reading the JCSP PIA and for compliments on the PIA.

You had a few questions about the PIA; as you are no doubt aware, my office and I do not usually answer questions in a one-off fashion from the public or advocates. With that said, since there appeared to be some confusion in the PIA, I wanted to provide some clarification to your questions.

First, DHS/US-CERT did not receive DIB company information from the CSPs during the DIB Pilot. With respect to the JCSP, US-CERT will receive anonymized information from the CSP about known or suspected cyber threats detected by the CSP. The CSP will identify the affected DIB company and provide additional information to US-CERT only if the CSP has been directed to do so by the DIB company. Information that US-CERT receives from the CSP is not expected to include PII. DIB companies may continue to share information with the Department of Defense under their existing relationship.

“Fact of occurrence” information provides DHS insights into which indicators have resulted in alerts. This information is useful in understanding what threat is being encountered and provides insight into the value of the indicator itself. Fact of occurrence does not identify which company was associated with the alert unless the participating DIB company has directed the CSP to share that information.

The CSP may provide information about IP addresses that are involved with actual or attempted cyber incidents. The CSP would only provide information in connection with an indicator that triggered an alert. Information that could be considered PII is included in an indicator shared with the CSPs as part of the JCSP will be positively associated with a known or suspected cybersecurity threat. No additional information that could be considered PII is expected to be shared by the CSPs back to the Government under this program.

I hope this clarifies the information in the PIA.

Hope you are doing well,
Best,
Mary Ellen

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)

Fax: (b) (6)
E-mail: (b) (6)
Website: www.dhs.gov/privacy

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 2:43 PM
To: Mary Ellen Callahan
Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII

found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW (b) (6)
Washington, DC 20006
(b) (6) direct
(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

Andrew, Emily

From: Andrew, Emily
Sent: Friday, January 20, 2012 9:50 PM
To: Goode, Brendan
Cc: Sand, Peter
Subject: RE: Question re JCSP PIA

I think that's awesome that someone wants to participate after seeing the PIA. Unfortunately, this is not our area, this is more of a program question, as I recall I read in one of our docs (maybe the SOC) that now new companies would be added for the pilot.

From: Goode, Brendan
Sent: Friday, January 20, 2012 4:48 PM
To: Andrew, Emily
Cc: Sand, Peter
Subject: RE: Question re JCSP PIA

An employee of (b)(4), (b)(7) asking about whether they could participate in the JCSP program. (b)(5)

Thanks,
Brendan

Office: (b)(6)
Blackberry: (b)(6)

From: Andrew, Emily
Sent: Friday, January 20, 2012 3:48 PM
To: Goode, Brendan
Cc: Sand, Peter
Subject: FW: Question re JCSP PIA

Brendan – regarding questions on the PIA, who did you receive the call from? And what type of questions were being asked?

Emily

From: Callahan, Mary Ellen
Sent: Friday, January 20, 2012 3:41 PM
To: Andrew, Emily
Cc: Sand, Peter
Subject: RE: Question re JCSP PIA

We don't usually answer questions on JCSP, if we have questions like that we often work with OPA to actually give the answer, even though we have the substance. Your OPA may just want to be on the call; I would recommend at least that as a response. Let me know the types of questions, so we have some visibility. Thanks! mec

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane SW, Mail Stop 0655

Washington, DC 20528-0655

Telephone: (b) (6)

Fax: (b) (6)

E-mail: (b) (6)

Website: www.dhs.gov/privacy

From: Andrew, Emily
Sent: Friday, January 20, 2012 3:21 PM
To: Callahan, Mary Ellen
Cc: Sand, Peter
Subject: FW: Question re JCSP PIA

Mary Ellen – I happy to have comments on the PIA directed to me but wanted to check with you first since your office is on the PIA. Let me know your preference.

Emily

From: Goode, Brendan
Sent: Friday, January 20, 2012 2:26 PM
To: McDermott, Thomas M; (b) (6) Andrew, Emily; (b) (6) (b) (6)
Cc: Falkenstein, Cindy; Sand, Peter
Subject: RE: Question re JCSP PIA

I received a phone call yesterday from someone that had read the JCSP PIA. Any general written guidance on how to respond to contact from outside?

Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: McDermott, Thomas M
Sent: Friday, January 20, 2012 2:25 PM
To: (b) (6) Andrew, Emily; Goode, Brendan; (b) (6)
Cc: Falkenstein, Cindy; Sand, Peter
Subject: RE: Question re JCSP PIA

(b) (5)

From: (b) (6)
Sent: Friday, January 20, 2012 2:00 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; (b) (6)
Cc: Falkenstein, Cindy; Sand, Peter
Subject: RE: Question re JCSP PIA

Emily –

Brendan's feedback is below. Otherwise, he believes this is good to go.

(b) (6)

(b) (6)
DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) 4 (BlackBerry)

From: Andrew, Emily

Sent: Thursday, January 19, 2012 3:56 PM

To: McDermott, Thomas M; Goode, Brendan; (b) (6)

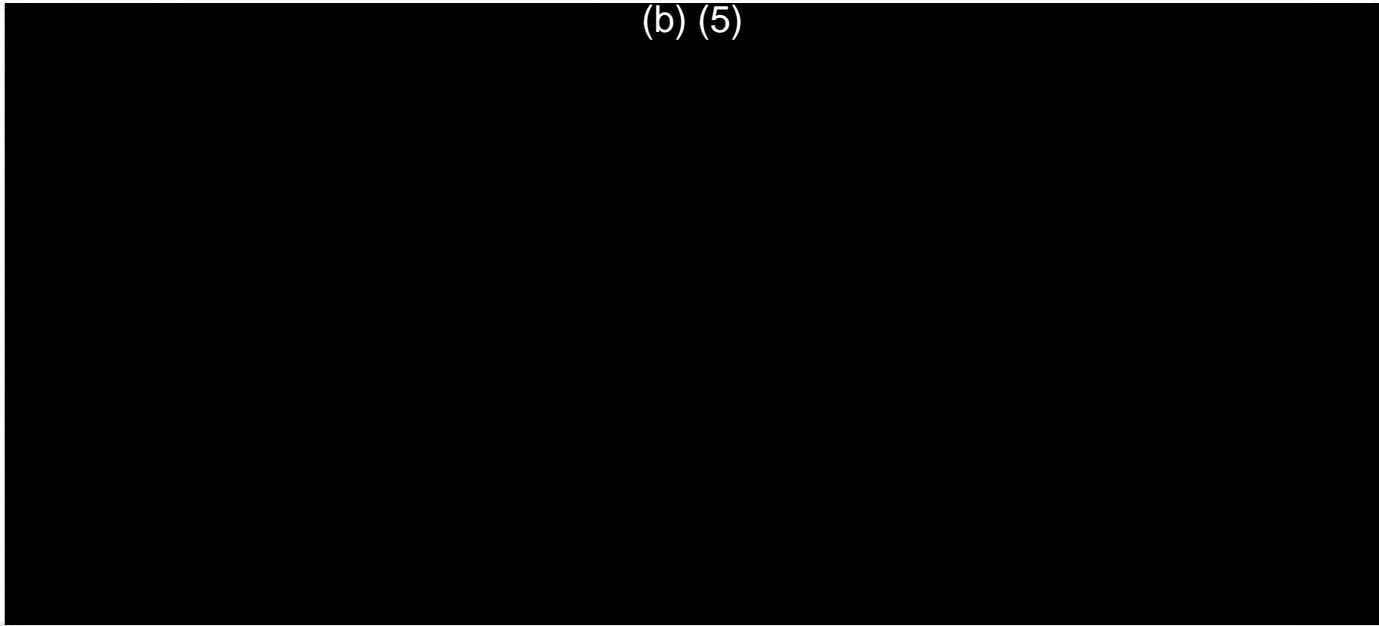
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)

Subject: RE: Question re JCSP PIA

Here's the latest draft response. Let me know if you are okay with this version or have any further edits. Also – since we kept this high level – let me know if we need to socialize with DoD and if so, who should we send it to.

Emily

(b) (5)



From: McDermott, Thomas M

Sent: Thursday, January 19, 2012 9:28 AM

To: (b) (6) Andrew, Emily

Cc: Goode, Brendan; Falkenstein, Cindy

Subject: RE: Question re JCSP PIA

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)

blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Thursday, January 19, 2012 9:04 AM
To: Andrew, Emily
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

Proposed updates to 1, 2, and 3 are below. (b) (5)
(b) (6) The PII is only used if it's directly related to a cyber threat (per US-CERT SOPs), so I'm not really sure what he's asking.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)
(b) (6) (Ballston Office)
(b) (6) 4 (BlackBerry)

From: Andrew, Emily
Sent: Thursday, January 19, 2012 6:41 AM
To: (b) (6)
Cc: Goode, Brendan; McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Question re JCSP PIA

(b) (6) – can you assist with responses from questions from CDT on the JCSP? (b) (5)
(b) (6) Once we have them reviewed by our team we can shoot them over to DoD to make sure they are okay with them as well.

Emily

The question is this:

1. What information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

(b) (5)

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:
IP address
Domain

Email header

Files

Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

2. If they don't contain PII, what does a "fact of" report actually contain?

(b) (5)

3. E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

(b) (5)

4. E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered?

(b) (5)

5. That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

(b) (5)

From: Goode, Brendan
Sent: Wednesday, January 18, 2012 6:43 PM
To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(b) (5)

Thanks,
Brendan

Office: (b) (6)
Blackberry: (b) (6)

From: Sand, Peter
Sent: Wednesday, January 18, 2012 3:03 PM
To: Callahan, Mary Ellen; Andrew, Emily; Goode, Brendan; (b) (6) McDermott, Thomas M; Landesberg, Martha
Subject: RE: Question re JCSP PIA

(adding Martha for awareness re: DPIAC)

From: Callahan, Mary Ellen
Sent: Wednesday, January 18, 2012 2:56 PM
To: Andrew, Emily; Sand, Peter; Goode, Brendan; (b) (6) McDermott, Thomas M
Subject: Fw: Question re JCSP PIA

(b) (5)

Predecisional

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (202) 258 9934

From: Greg Nojeim (b) (6)
Sent: Wednesday, January 18, 2012 02:43 PM
To: Mary Ellen Callahan (b) (6)

Subject: Question re JCSP PIA

Hi Mary Ellen, and happy new year! I hope you had some time to relax during the holidays....

I'm writing today with a very specific question about the JCSP PIA released on January 13, http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. But, before I ask the question, kudos for doing the PIA: it explains the information sharing that occurred in the DIB Pilot and that will occur going forward, better than any document of which I am aware that is in the public domain.

The question is this: what information did the companies that participated in the DIB Pilot, and what information could the companies that participate in the JCSP, report back to U.S. CERT?

The PIA indicates that "threat indicators" are/will be shared by the government to Communication Service Providers. The indicators can be used to create intrusion detection signatures. The indicators fall into five categories:

- IP address
- Domain
- Email header
- Files
- Strings

An "indicator report" consists of one or more indicators grouped together and submitted. An indicator report could include one email, one file and one domain, or four files, two domains and three IP addresses.

When a CSP develops a signature from threat indicators provided by US-CERT, and it gets a hit on that signature, the CSP may voluntarily send U.S. CERT "information related to cyber threat indicators or other possible known or suspected cyber threats." PIA p. 3. "CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII." PIA p. 4. The PIA repeats this a few times -- that CSPs may share information about known or suspected cyber threats they have detected, but the "fact of" information does not contain PII.

If they don't contain PII, what does a "fact of" report actually contain?

E.g.: DHS took the position in an Einstein PIA that IP address is not PII. Can the info a CSP reports back include IP address?

E.g.: if a CSP develops a signature based on threat indicators provided by US CERT, and those threat indicators do contain PII as might be found in an email header, and/or IP address, doesn't a report back that the signature was detected implicitly disclose that the PII found in the header, or the IP address, was encountered? That is, even if the "fact of" information that is reported does not include PII, doesn't the reporting of the "fact of" information disclose that the PII that was part of the threat indicator was encountered, even though it is not re-disclosed to US CERT?

-- Greg

Gregory T. Nojeim
 Senior Counsel and
 Director, Project on Freedom, Security & Technology
 Center for Democracy & Technology
 1634 Eye St., NW (b) (6)
 Washington, DC 20006
 (b) (6) direct

00078

(b) (6) fax
(b) (6)

Follow our Security and surveillance work on Twitter at @CDT_Security.

From: [Andrew, Emily](#)
To: [Sand, Peter](#)
Cc: [Falkenstein, Cindy](#)
Subject: FW: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60
Date: Tuesday, January 24, 2012 7:26:56 AM

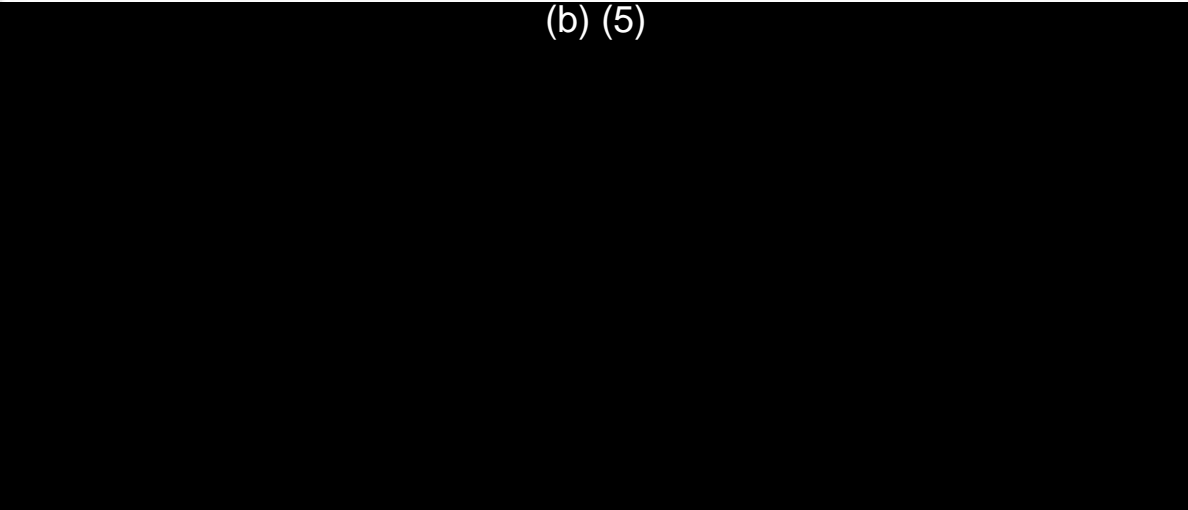
Pete – Cindy and I have reviewed the document and have no comments or changes.

Thanks for looping us in on the review.

Emily

From: McDermott, Thomas M
Sent: Monday, January 23, 2012 4:37 PM
To: Andrew, Emily; Goode, Brendan
Cc: (b) (6) Falkenstein, Cindy; Sand, Peter
Subject: RE: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

(b) (5)



Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Andrew, Emily
Sent: Sunday, January 22, 2012 8:24 AM
To: McDermott, Thomas M; Goode, Brendan
Cc: (b) (6) Falkenstein, Cindy; Sand, Peter
Subject: FW: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

Tom/Brendan,

I'm forwarding this because I don't want to assume that you've seen or had the opportunity to review the attached DOD - Final Rule on DIB Activities. It appears that the (b) (5) To Pete's questions below,

(b) (5)

Thanks,
Emily

From: Sand, Peter
Sent: Friday, January 20, 2012 12:59 PM
To: Landesberg, Martha; Foster, Helen; Mathews, Scott; Andrew, Emily; Falkenstein, Cindy; Rebecca J. Richards (b) (6)
Cc: PRIV Exec Sec; Gottfried, Jordan
Subject: RE: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

Emily, Becky, Helen,

This is a DOD "Rule" related to Cyber that's all about information sharing - so I'm looking to you guys to figure out who else should review it - comments due back Tuesday.

I marked sections that got my attention... did not put comments in the doc.

(b) (5)

(b) (5)

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security

(b) (6)

(b) (6)

www.dhs.gov/privacy

Join lively discussions with outside experts!

The DHS Privacy Office Speaker Series
(open to all federal employees and contractors)

<http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm>

Reserve your spot in the front row! (b) (6)

From: Landesberg, Martha

Sent: Tuesday, January 17, 2012 9:17 PM

To: Foster, Helen; Mathews, Scott

Cc: PRIV Exec Sec; Gottfried, Jordan; Sand, Peter

Subject: FW: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

This is DOD information sharing for your review. I will coordinate response, and Pete should also weigh in, but think the two of you may have insights – I think there are a least “derivative” PRIV equities here....

tx

Martha K. Landesberg
Associate Director, Privacy Policy
Privacy Office
Department of Homeland Security
Phone: (b) (6)
Fax: (b) (6)

From: PRIV Exec Sec

Sent: Tuesday, January 17, 2012 4:52 PM

To: Sand, Peter; Landesberg, Martha
Cc: Gottfried, Jordan
Subject: FW: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

Good afternoon,

Please see the attached report that requires comments/clearance by **3pm on January 24**. If applicable, please ensure internal coordination prior to submission to PRIV Exec Sec. Thank you.

From: (b) (6)
Sent: Tuesday, January 17, 2012 1:23 PM
To: OGC Regulatory Affairs; OGC Regs - Atty Circulation
Cc: OGC HQS RLD; DHS Regulations
Subject: Interagency Rule for Review: Due COB Tues 1/24 - DOD Interim Final Rule - Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities - 0790-AI60

Available for your review, is a DOD Interim Final Rule titled "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities."

Deadline. By **COB Tuesday Jan 24**, please send all comments to (b) (6) and please Cc (b) (6) OGC Reviewers: Please insert your comments into the version on the OGC shared drive, per the instructions below.

Summary of Rule. DoD is publishing an interim final rule to establish a voluntary cyber security information sharing program between DoD and eligible cleared defense contractors. The program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

Point of Contact. If your component submits comments, please include a point of contact (POC) – including a name and phone number – with your comments. The POC should be able to discuss the substance of the comments or to identify individuals in your component who can discuss the substance. OGC will contact the POC if we have follow-up questions.

OGC Reviewers. Please insert your comments into the document, titled (b) (5) which is located at (b) (7)(E) and please notify (b) (6) after you insert your comments. Do not insert your comments into the attached document.

Authorization for Sharing. Do not share this rule, in whole or in part, with anyone outside of DHS without first obtaining authorization for such disclosure from the DHS OGC Regulatory Affairs Law Division.

Thank you.

(b) (6)

Legal Administrative Specialist, Regulatory Affairs
Office of the General Counsel
U.S. Department of Homeland Security

(b) (6) (office)

(b) (6) (BB)

(b) (6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

Andrew, Emily

From: Falkenstein, Cindy
Sent: Tuesday, February 07, 2012 8:45 AM
To: Andrew, Emily
Subject: RE: DIB/JCSP Final recommendations. from AM review

Importance: High

Emily,

(b) (5)

Give me a call so we can discuss further if you wish.
I did not respond with any edits to the document on the HIGH side.

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | ☎ (b) (6) (O) | 📠 (b) (6) (BB) |
✉ (b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: Andrew, Emily
Sent: Tuesday, February 07, 2012 6:53 AM
To: McDermott, Thomas M
Cc: Falkenstein, Cindy
Subject: Final recommendations.

Hi Tom – can you let me know your availability for a call to discuss the final recommendations and way forward? I’m open today between 1130 – 1 and then tomorrow morning.


Thanks
Emily

Emily Andrew, CIPP, CIPP/G | Sr. Privacy Officer
National Protection and Programs Directorate | U.S. Department of Homeland Security
1616 N. Ft. Myer Dr. (b) (6) | Arlington VA 22209 | ☎ (b) (6) | 📠 (b) (6)

Falkenstein, Cindy

From: Falkenstein, Cindy
Sent: Tuesday, February 07, 2012 8:58 AM
To: Richards, Rebecca; (b) (6) (CTR); Sand, Peter; Andrew, Emily; (b) (6)
(b) (6) Steiner, Kurt
Cc: Goode, Brendan; Eberle, Carole; Falkenstein, Cindy
Subject: NCPS Privacy Compliance Workgroup Minutes: Monday, February 6, 2012

(b) (5)



Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: [Falkenstein, Cindy](#)
To: [Andrew, Emily](#)
Subject: docs on high side: E3 & JCSP/DIB
Date: Wednesday, February 15, 2012 12:46:00 PM

Emily,

I've gone through my mail up on the high side, and found two emails from (b) (6) that are of interest for the E3 PIA. (b) (6) me the (b) (5) so I will follow up with Mark to see if that is the latest version.) He also sent some E3 Training from one of their vendors up at the Fort; I have not gone into each of the attachments to review (no comments requested), but wanted to let you know he sent them to me.

(b) (5)

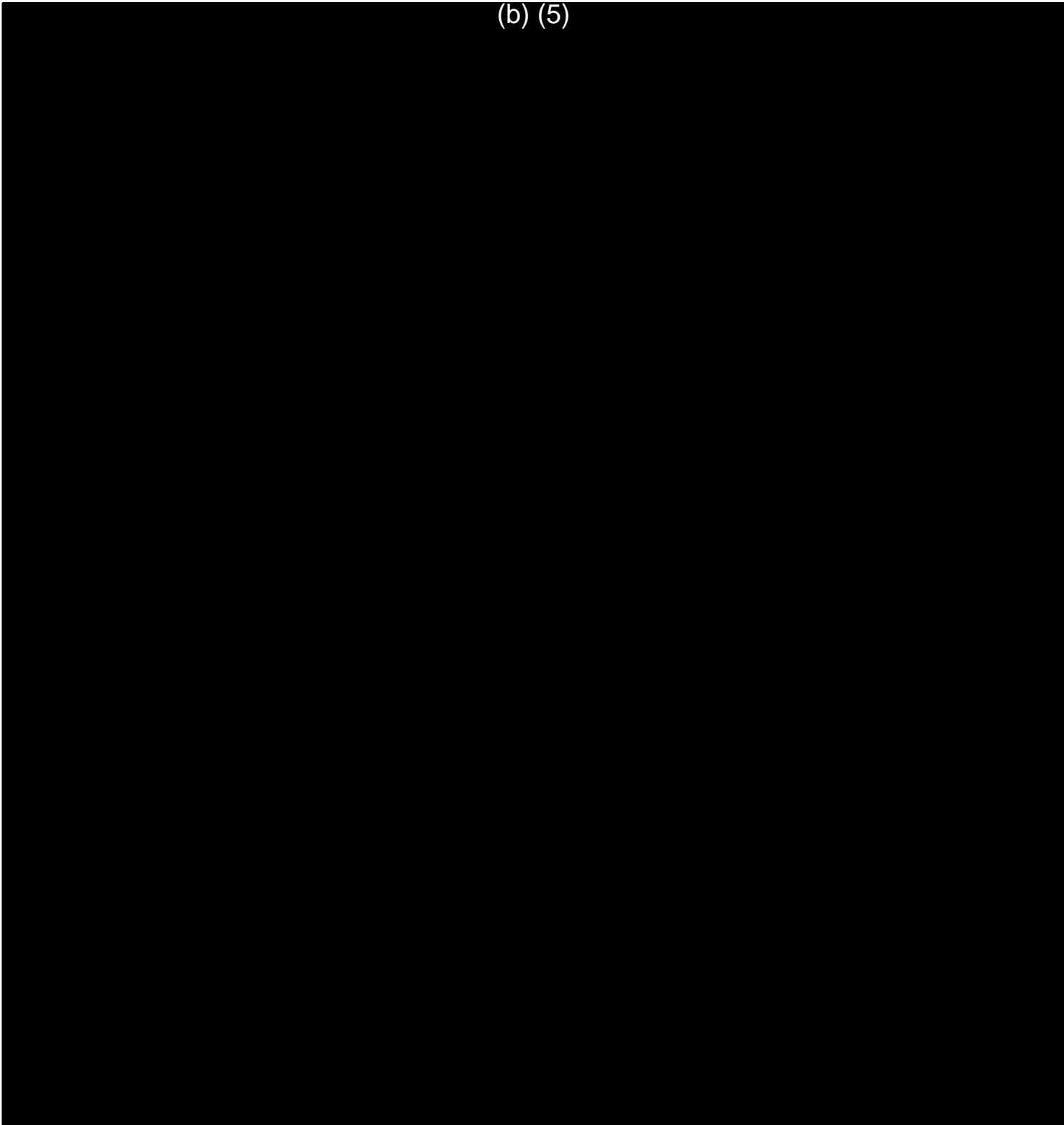
Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

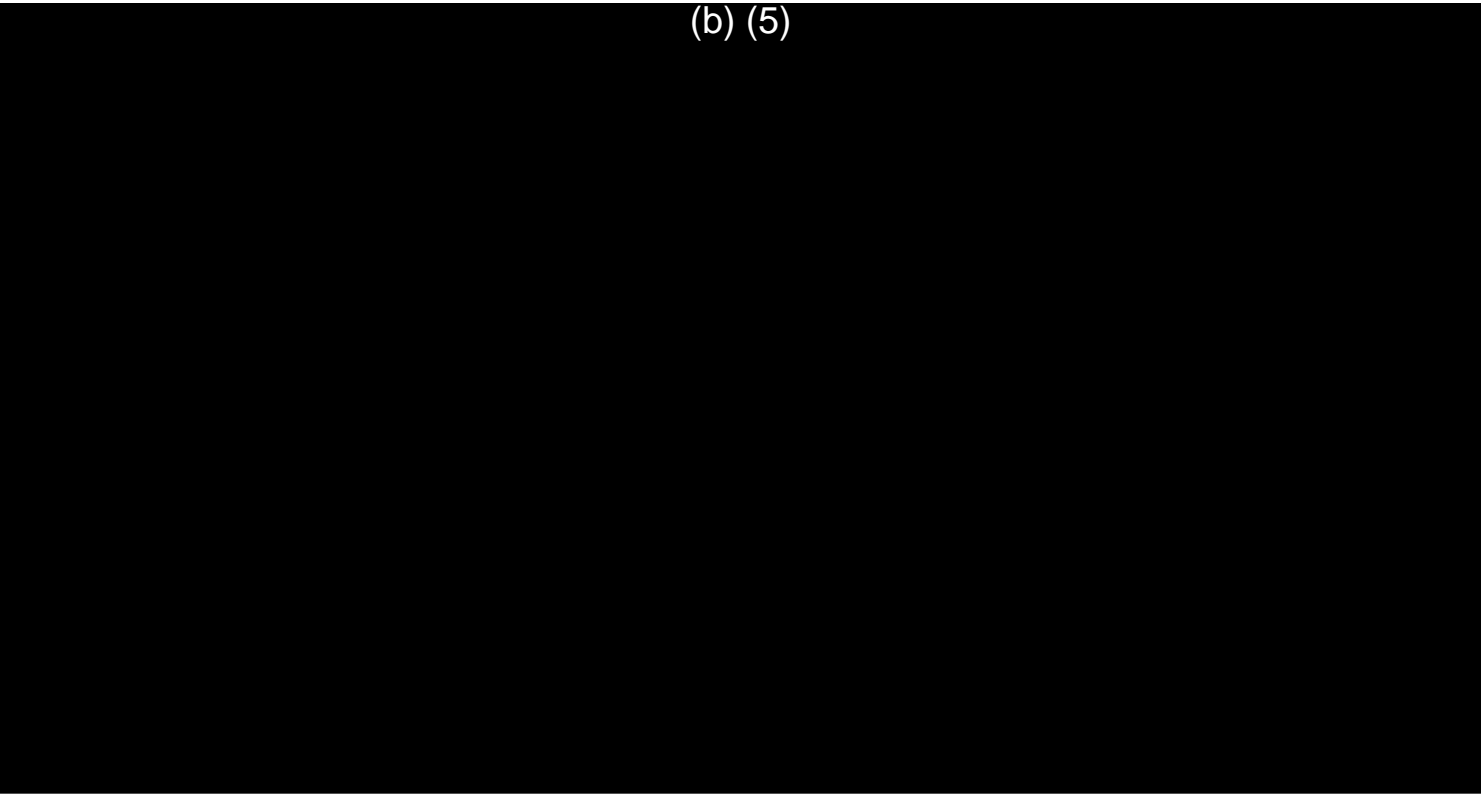
Andrew, Emily

From: Falkenstein, Cindy
Sent: Monday, March 12, 2012 10:00 AM
To: Andrew, Emily; (b) (6); (b) (6); Steiner, Kurt; Sand, Peter; (b) (6)
Cc: Richards, Rebecca; Goode, Brendan; Falkenstein, Cindy; Eberle, Carole
Subject: NCPS Privacy Compliance Workgroup Minutes: Monday, March 5, 2012
Attachments: NCPS Privacy Compliance Workgroup Minutes: Monday, February 6, 2012; DPIAC_Cybers
Sub_Agenda_March 8_FINAL_03072012.docx

(b) (5)



(b) (5)



**CYBER SUBCOMMITTEE****DATA PRIVACY & INTEGRITY ADVISORY COMMITTEE****March 8, 2012, 3:00 p.m. – 5:00 p.m.****(b) (6) 9th Floor, 1110 North Glebe Road, Arlington, VA 22201****Welcome and Update** 3:00 p.m. – 3:15 p.m.

- Dan Chenok
IBM Global Business Services

Joint Cyber Program and Cyber Pilots Overview 3:15 p.m. – 4:00 p.m.

- Brendan Goode
Director, National Cyber Security Division
- Mark White
Cyber Pilot Program Director

Report Status Update: Current tasking 4:00 p.m. – 5:00 p.m.

- Dan Chenok
IBM Global Business Services

Closing Remarks 5:00 p.m.

From: [Andrew, Emily](#)
To: [Sand, Peter](#)
Cc: [Richards, Rebecca](#); [Callahan, Mary Ellen](#); [Falkenstein, Cindy](#); [Foster, Helen](#)
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)
Date: Wednesday, March 21, 2012 12:43:15 PM
Attachments: [MARCH 2012v3.doc](#)

Thanks in looking at this again – the review expands the conversation into the JCSP. I think the only challenge we really had for the JCSP was the time frame to get the PIA completed. (b) (5)

[REDACTED]

[REDACTED]

(b) (5)

[REDACTED]

From: Sand, Peter
Sent: Wednesday, March 21, 2012 12:33 PM
To: Andrew, Emily
Cc: Richards, Rebecca; Callahan, Mary Ellen; Falkenstein, Cindy; Foster, Helen
Subject: Re: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

Emily,

No- I don't recalling [REDACTED] (b) (5)

Only thing [REDACTED] (b) (5)

[REDACTED]

Pete

Peter E. Sand | DHS PRIV | [REDACTED] (b) (6)

Sent via blackberry. Please excuse the effects of big thumbs on little keys.

From: Andrew, Emily
Sent: Wednesday, March 21, 2012 12:25 PM
To: Sand, Peter
Cc: Richards, Rebecca; Callahan, Mary Ellen; Falkenstein, Cindy
Subject: FW: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

Pete – NSD is working on the responses to questions from the GAO in prep for a call tomorrow on the DIB Pilot – the question is as follows:

1. To what extent has DHS encountered any challenges such as any privacy or legal concerns while operating the Opt-In Cyber Pilot? Please explain. [\[d1\]](#)

(b) (5)

Emily

From: (b) (6)
Sent: Wednesday, March 21, 2012 11:15 AM
To: McDermott, Thomas M; (b) (6) Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan; (b) (6) (b) (6) Eberle, Carole
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)
Importance: High

OGC and Privacy,

We are working on the responses to the questions on the DIB Pilot from GAO in preparation for the call tomorrow. We specifically need input from you for the following:

1. OGC: Questions 4, 5, 7, 8
2. Privacy: Question 8

As the call is tomorrow, I need answers as soon as you can reasonably provide them today. My apologies for the short turn around request.

Thanks,

(b) (6)

From: Eberle, Carole
Sent: Wednesday, March 14, 2012 1:30 PM
To: (b) (6) McElroy, Deron T; Odderstol, Thad; (b) (6) Rock, Lee; Harris, Richard; (b) (6) Glick, Jeffrey; (b) (6) (b) (6) Schneider, Eric
Cc: (b) (6) (b) (6) Menna, Jenny; Hanson, Eric; Shabat, Matthew; McElroy, Deron T; Goode, Brendan; (b) (6) NSD Exec Sec; NCS Exec Sec; McDermott, Thomas M; (b) (6) Royster, Kristin
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

All - the meeting with GAO is set for March 22nd from 2:00 – 3:00 in conference room 729 (I'm also working on getting a conference bridge). I have a POC from NSD, and will need one from CICPA, US-CERT and maybe NCCIC (Eric?) and possibly NCS (Jeff?). Please let me know who the POC is so I can send the invite. If possible, please respond to the questions by 1200 on Tuesday, 3/20 and return them to me.

Thank you,
Carole

From: Eberle, Carole
Sent: Wednesday, March 07, 2012 5:30 PM
To: Goode, Brendan; (b) (6); (b) (6); McDermott, Thomas M; (b) (6)
McElroy, Deron T; Odderstol, Thad; (b) (6); Rock, Lee; Harris, Richard; (b) (6)
Cc: (b) (6); (b) (6); Menna, Jenny; Hanson, Eric; Shabat, Matthew
Subject: FW: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

All,

Some of you spoke with (b) (5) (b) (5)
(b) (5)

(b) (5) so please let me know what days work best for you during Mar 22, 23, 26, 27, 28 and 29. If we can have written responses several days before the call, it will help to ensure we are all on the same page. I will also work on setting up an internal call so we can discuss before talking to GAO.

Please let me know if you have questions.

Thank you,
Carole

From: [Andrew, Emily](#)
To: [Andrew, Emily](#); (b) (6); [McDermott, Thomas M](#); (b) (6); [Falkenstein, Cindy](#)
Cc: [Goode, Brendan](#); (b) (6); (b) (6); [Eberle, Carole](#); [Sand, Peter](#)
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)
Date: Wednesday, March 21, 2012 12:49:26 PM

(b) (6)

In looking at this again – the review expands the conversation into the JCSP. I think the only challenge we really had for the JCSP was the time frame to get the PIA completed. (b) (5)

(b) (5)

(b) (5)

Emily

From: Andrew, Emily
Sent: Wednesday, March 21, 2012 12:31 PM
To: (b) (6); [McDermott, Thomas M](#); (b) (6); [Falkenstein, Cindy](#)
Cc: [Goode, Brendan](#); (b) (6); (b) (6); [Eberle, Carole](#); [Sand, Peter](#)
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

(b) (6) for PRIV – you meant Question #7 correct? Also – is this strictly for the DIP Pilot – not related to JCSP?

Emily

From: (b) (6)
Sent: Wednesday, March 21, 2012 11:15 AM
To: [McDermott, Thomas M](#); (b) (6); [Andrew, Emily](#); [Falkenstein, Cindy](#)
Cc: [Goode, Brendan](#); (b) (6); (b) (6); [Eberle, Carole](#)
Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)
Importance: High

OGC and Privacy,

We are working on the responses to the questions on the DIB Pilot from GAO in preparation for the call tomorrow. We specifically need input from you for the following:

1. OGC: Questions 4, 5, 7, 8
2. Privacy: Question 8

As the call is tomorrow, I need answers as soon as you can reasonably provide them today. My apologies for the short turn around request.

Thanks,

(b) (6)

From: Eberle, Carole

Sent: Wednesday, March 14, 2012 1:30 PM

To: (b) (6) McElroy, Deron T; Odderstol, Thad; (b) (6) Rock, Lee; Harris, Richard; (b) (6) Glick, Jeffrey; (b) (6) (b) (6) Schneider, Eric

Cc: (b) (6) (b) (6) Menna, Jenny; Hanson, Eric; Shabat, Matthew; McElroy, Deron T; Goode, Brendan; (b) (6) NSD Exec Sec; NCS Exec Sec; McDermott, Thomas M; (b) (6) Royster, Kristin

Subject: RE: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

All - the meeting with GAO is set for March 22nd from 2:00 – 3:00 in conference room 729 (I'm also working on getting a conference bridge). I have a POC from NSD, and will need one from CICPA, US-CERT and maybe NCCIC (Eric?) and possibly NCS (Jeff?). Please let me know who the POC is so I can send the invite. If possible, please respond to the questions by 1200 on Tuesday, 3/20 and return them to me.

Thank you,
Carole

From: Eberle, Carole

Sent: Wednesday, March 07, 2012 5:30 PM

To: Goode, Brendan; (b) (6) (b) (6) McDermott, Thomas M; (b) (6) McElroy, Deron T; Odderstol, Thad; (b) (6) Rock, Lee; Harris, Richard; (b) (6)

Cc: (b) (6) (b) (6) Menna, Jenny; Hanson, Eric; Shabat, Matthew

Subject: FW: GAO Review on DOD's Efforts for Protecting the Defense Industrial Base From Cyber Threats (351656)

All,

Some of you spoke with (b) (5) (b) (5)

(b) (5)

GAO would like a con call with us to discuss the answers so please let me know what days work best for you during Mar 22, 23, 26, 27, 28 and 29. If we can have written responses several days before the call, it will help to ensure we are all on the same page. I will also work on setting up an internal call so we can discuss before talking to GAO.

Please let me know if you have questions.

Thank you,
Carole

From: [Andrew Emily](#)
To: [NPPDPrivacy](#)
Subject: FW: Process flow map: NCSD: .com to DHS
Date: Monday, March 28, 2011 2:48:34 PM
Attachments: [PA DIB Pilot Briefing Card 2011-03-17.doc](#)
Importance: High

Another project. We can label as DIB Pilot.

-----Original Message-----

From: Sand, Peter
Sent: Friday, March 25, 2011 12:11 PM
To: Andrew, Emily
Cc: (b) (6)
Subject: Process flow map: NCSD: .com to DHS
Importance: High

Emily,

I think we need a (b) (5)

(b) (5)

It will also frame the individual discussion we've been having about the fly away teams, etc.

Thoughts?

Pete

Peter E. Sand, J.D., CIPP/G-IT
Director of Privacy Technology
Department of Homeland Security
voice: (b) (6) pager (b) (6) (b) (6) www.dhs.gov/privacy

-----Original Message-----

From: Sand, Peter
Sent: Friday, March 25, 2011 11:28 AM
To: Mary Ellen Callahan (b) (6); John W. Kropf (b) (6)
Emily Andrew (b) (6)
Subject: DIB Pilot Starting and Branded as a DHS program
Importance: High

MEC,

See below from RADM Brown. I'll find out timing and exactly what DHS's role is - (b) (5)

From: Andrew, Emily
Sent: Thursday, May 10, 2012 12:50 PM
To: Sand, Peter; (b) (6) Richards, Rebecca
Cc: Falkenstein, Cindy
Subject: fw: JCSP-DIB
Attachments: 20120509 DIB Fact Sheet v6 (FINAL CLEAN) (3)_PRIVedits 20120510.docx; 20120509 FINAL DRAFT DIB ECSS Comms Plan v5 (OSD Final CLEAN) (2)_PRIV20120510.docx

FYI – I'm not sure why the (b) (5)
and I think we should recognize that.

(b) (5)

Emily

From: Andrew, Emily
Sent: Thursday, May 10, 2012 12:39 PM
To: Davis, Robert M
Cc: McDermott, Thomas M; (b) (6)
Subject: FW: JCSP - DIB

Bob – I know these are listed as final draft but I have a few comments / edits redline on the attached for your consideration.

(b) (5)

I've copied Tom McDermott for his input on this as well.

Thanks,
Emily

From: Davis, Robert M
Sent: Thursday, May 10, 2012 10:10 AM
To: Andrew, Emily
Subject: RE: JCSP - DIB

Here you go.

(b) (7)(E)

7/5/2012

From: Andrew, Emily
Sent: Thursday, May 10, 2012 10:01 AM
To: Davis, Robert M
Subject: JCSP - DIB

Bob – can you send me a copy of the latest draft communications discussed this morning?

Thanks
Emily

Emily Andrew, CIPP, CIPP/G | Sr. Privacy Officer
National Protection and Programs Directorate | U.S. Department of Homeland Security
1616 N. Ft. Myer Dr. (b) (6) | Arlington VA 22209 | (b) (6) (b) (6)

From: Falkenstein, Cindy
Sent: Wednesday, May 16, 2012 4:01 PM
To: Andrew, Emily
Subject: JCSP/DECS DRaft PIA
Attachments: Initial DHS NPPD DESC PIA 051412_cvf.doc

Emily,

Attached is my first attempt at a rough draft for the JCSP/DESC PIA. I had intended to provide this to you yesterday as requested, however, due to the reprioritization of the TAF information, the initial draft for a new PIA was pushed back.

I have taken today to review all of the information you provided recently for the JCSP/DIB ESC (DESC), and input changes where might be appropriate. (b) (5)

Also in the interest of time, I have not proof-read this version as it is the initial draft; and as PIAs will normally take months to fine-tune, I wanted to get this started so we can make edits and tweak the language/details as we progress.

I hope this is what you were expecting; if not please provide me your thoughts.

Cindy

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

"Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all."

— [Dale Carnegie](#)

From: [Andrew, Emily](#)
To: [Sand, Peter](#)
Cc: [Falkenstein, Cindy](#); (b) (6)
Subject: RE: JCSP In the news - "strict privacy protections"
Date: Friday, May 18, 2012 8:54:08 AM
Attachments: [Privacy Oversight DHS task 20111219.docx](#)

DOD has the (b) (5)

(b) (5)
There may be a more updated version – just need to check my files. Is this what you had in mind?

From: Sand, Peter
Sent: Friday, May 18, 2012 7:51 AM
To: Andrew, Emily; Falkenstein, Cindy; (b) (6)
Subject: JCSP In the news - "strict privacy protections"

All,

Reading Ellen Nakashima's piece in the Post:
http://www.washingtonpost.com/world/national-security/pentagon-to-expand-cybersecurity-program-for-defense-contractors/2012/05/11/gIQALhjbHU_story.html

"The companies may turn over results of the screening to the government. The data would go to DHS and could be shared with agencies such as the NSA and FBI, but with strict privacy protections, officials said."

I recall from the OPA materials that DOD is taking the lead on privacy questions...

Is that right? Or are we handling the OPA piece for our portion and DOD for theirs?

Let's write something up that lists the "strict privacy protections" – just to have that ready.

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
The Privacy Office, Department of Homeland Security
(b) (6) | (b) (6) | www.dhs.gov/privacy

Re Privacy meeting on Brendan's calendar today

From: Andrew, Emily
Sent: Monday, May 21, 2012 9:24 AM
To: (b) (6) Falkenstein, Cindy; (b) (6)
Cc: (b) (6)
Subject: Re: Privacy meeting on Brendan's calendar today

(b) (6)

I'm not sure but it could be (b) (5)

(b) (5)

I'm copying (b) (6), MEC's Executive Assistant and (b) (6) for any additional input.

Emily

Emily Andrew
Senior Privacy Officer
DHS/NPPD
(b) (6)

----- Original Message -----

From: (b) (6)
Sent: Monday, May 21, 2012 02:09 PM
To: Falkenstein, Cindy; Andrew, Emily
Subject: Privacy meeting on Brendan's calendar today

Cindy/Emily -

There's a meeting hold on Brendan's calendar today from 3-4. Did you guys set that up?

If so, what's the context? Laura was asking me to cover this morning, as Brendan has a conflict, and it's the first I've heard of it.

If this isn't your meeting, just let me know and I'll do some more digging.

Thanks!
(b) (6)

From: (b) (6)
Sent: Thursday, May 24, 2012 9:13 AM
To: Falkenstein, Cindy; Lockett, Vania
Cc: NPPDPrivacy
Subject: RE: NCPS JCSP DESC Update PIA
Attachments: NPPD JCSP DESC PIA Update 052112 cvf (RJF 0524 12).docx

Hi Cindy,

Please find my comments to the NCPS JCSP DECS Update PIA. Most comments were too global to provide in-line edits.

(b) (5)

Also, I checked the DHS PRIV website and there is a new PIA Update template available. Under the properties is has April 2012 as the document date; I think this is the correct template.

Please let me know if you would like to discuss further.

Thanks,

(b) (6)

(b) (6), CIPP/US, CIPP/G, CISSP
Senior Privacy Analyst | National Protection and Programs Directorate | U.S. Department of Homeland Security
(b) (6) (O) | (b) (6) (BB) | Privacy Website | NPPD Privacy Intranet

From: Falkenstein, Cindy
Sent: Wednesday, May 23, 2012 1:16 PM
To: Lockett, Vania; (b) (6)
Cc: NPPDPrivacy
Subject: FW: NCPS JCSP DESC Update PIA

Hi Vania (b) (6)

Just following up on the NPPD JCSP DESC PIA update. I don't mean to put any additional pressure on you, as I know you're all just as busy as I am, but I was under the impression that (b) (5)

(b) (5)

Would

it be possible to give me an indication as to when we might be able to send this over to NSD for their review? Can you let me know what next steps I might be able to assist you with?

Thanks,
Cindy

Cindy Falkenstein

Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

“Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all.”

— [Dale Carnegie](#)

From: Falkenstein, Cindy
Sent: Monday, May 21, 2012 9:59 AM
To: (b) (6) Lockett, Vania
Cc: Andrew, Emily; Falkenstein, Cindy
Subject: RE: NCPS JCSP DESC Update PIA

Vania, (b) (6)

I have reviewed Emily’s version, and made some changes to reflect her comments. Please review and let me know what additional comments/edits you would like to make. As noted in Emily’s email, once we have another version that we feel comfortable with, I will pass along to NSD for further dissemination.

Thanks,
Cindy

Cindy Falkenstein

Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

“Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all.”

— [Dale Carnegie](#)

From: Andrew, Emily
Sent: Sunday, May 20, 2012 9:50 AM
To: Falkenstein, Cindy
Cc: (b) (6) Lockett, Vania
Subject: RE: NCPS JCSP DESC Update PIA

Cindy – (b) (5). I’ve provide some general comments, redlined on the attached, for the most part we need to focus on DHS role and the changes from the JCSP to the DECS, which are limited. Cindy – I agree with your comment that we need to verify the info sharing.

All once we have another version that you all feel comfortable with, please send to Brendan, OGC and team through either (b) (6) (if she is back) or Ken Kraper.

Thanks
Emily

Emily Andrew, CIPP, CIPP/G | Sr. Privacy Officer
National Protection and Programs Directorate | U.S. Department of Homeland Security
1616 N. Ft. Myer Dr. (b) (6) | Arlington VA 22209 | (b) (6) | (b) (6)

From: Falkenstein, Cindy
Sent: Friday, May 18, 2012 4:49 PM
To: Andrew, Emily
Subject: FW: NCPS JCSP DESC Update PIA

I have also posted the update PTA to the NPPD shared drive at:

(b) (7)(E)

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
c (b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

“Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all.”
— Dale Carnegie

From: Falkenstein, Cindy
Sent: Friday, May 18, 2012 4:42 PM
To: Andrew, Emily
Cc: Falkenstein, Cindy
Subject: NCPS JCSP DESC Update PIA

Emily,
Please review this Update PIA for JESP DECS, and let me know if you have any additional comments before taking any further actions.

I have used the (b) (5)
however, I would appreciate you noting any errors you may find, and to please bring them to my attention so that I may correct them immediately so we may send the most up-to-date version to the PM for their review and input, prior to submitting to DHS HQ PRIV.

As promised, by COB today.
Thank you,
Cindy

Cindy Falkenstein

Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

“Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all.”
— [Dale Carnegie](#)

Andrew, Emily

From: (b) (6) (b) (6)
Sent: Tuesday, January 17, 2012 6:42 PM
To: Callahan, Mary Ellen; Goode, Brendan
Cc: (b) (6) Andrew, Emily
Subject: RE: JCSP PIA

Terrific, thanks for the quick update (and citation to the final version).

From: Callahan, Mary Ellen (b) (6)
Sent: Tuesday, January 17, 2012 6:32 PM
To: Silk, Jennifer; (b) (6)
Cc: (b) (6) (b) (6) Andrew, Emily
Subject: Re: JCSP PIA

Hi there, yes, both DOD and NSA reviewed the PIA before it became public. (b) (5)
[Redacted]

The PIA was posted this morning on the dhs privacy site, I believe at:
http://www.dhs.gov/files/publications/gc_1284567214689.shtm

(Working off my bberry, but I think the citation is correct).

Thanks, please let me know if you have additional questions. Mec.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: Silk, Jennifer (b) (6)
Sent: Tuesday, January 17, 2012 06:27 PM
To: Goode, Brendan; Callahan, Mary Ellen
Cc: (b) (6)
Subject: JCSP PIA

Good evening,
Can you please tell me if the JCSP PIA was reviewed by DOD/NSA, specifically to review for classification regarding the description of the countermeasures in the overview section? Further, want to be sure the abstract and overview describe the activities consistent with joint messages between the departments to DIB companies and others and with the DC SOC. Has this been posted online yet?

Thanks,
(b) (6)

(b) (6)
Director, Cybersecurity

00107

National Security Staff
The White House

(b) (6)

(b) (6) (direct)

(b) (6) (secure)

From: [Andrew, Emily](#)
To: [Sand, Peter](#); [Falkenstein, Cindy](#)
Subject: FW: JCSP PIA
Date: Wednesday, January 18, 2012 6:17:31 AM

FYI – only.

From: (b) (6); (b) (6)
Sent: Tuesday, January 17, 2012 6:42 PM
To: Callahan, Mary Ellen; Goode, Brendan
Cc: (b) (6); Andrew, Emily
Subject: RE: JCSP PIA

Terrific, thanks for the quick update (and citation to the final version).

From: Callahan, Mary Ellen; (b) (6)
Sent: Tuesday, January 17, 2012 6:32 PM
To: (b) (6); Goode, Brendan
Cc: (b) (6); Andrew, Emily
Subject: Re: JCSP PIA

Hi there, yes, both DOD and NSA reviewed the PIA before it became public. (b) (5)

[REDACTED]

The PIA was posted this morning on the dhs privacy site, I believe at:
http://www.dhs.gov/files/publications/gc_1284567214689.shtm

(Working off my bberry, but I think the citation is correct).

Thanks, please let me know if you have additional questions. Mec.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Work: (b) (6)
Cell: (b) (6)

From: (b) (6); (b) (6)
Sent: Tuesday, January 17, 2012 06:27 PM
To: Goode, Brendan; Callahan, Mary Ellen
Cc: (b) (6); (b) (6)
Subject: JCSP PIA

Good evening,
Can you please tell me if the JCSP PIA was reviewed by DOD/NSA, specifically to review for

classification regarding the description of the countermeasures in the overview section? Further, want to be sure the abstract and overview describe the activities consistent with joint messages between the departments to DIB companies and others and with the DC SOC. Has this been posted online yet?

Thanks,

(b) (6)

(b) (6)

Director, Cybersecurity
National Security Staff
The White House

(b) (6)

(b) (6) (direct)

(b) (6) (secure)

From: McDermott, Thomas M
Sent: Monday, January 30, 2012 2:50 PM
To: Goode, Brendan; (b) (6) Rock, Lee; Harris, Richard; Falkenstein, Cindy
Cc: Stempfley, Roberta
Subject: FW: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

I'm not sure who is tracking these requirements for CS&C/NCSD.

(b) (5)

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6) (b) (6)
Sent: Monday, January 23, 2012 7:03 PM
To: Schaffer, Gregory; Rosenbach, Eric; (b)(6)-P.L. 86-36; (b) (6) (b) (6) Stempfley, Bobbie (b) (6)
McConnell, Bruce; (b) (6) McDermott, Thomas M; Goode, Brendan; (b) (6)
(b) (6)
Subject: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

All,

(b) (5)

(b) (5)

Thank you,

(b) (6)

(b) (6)

Director, Cybersecurity
National Security Staff
The White House

(b) (6)

(b) (6) direct

(b) (6) (secure)

From: [McDermott, Thomas M](#)
To: [McDermott, Thomas M](#); [Goode, Brendan](#); [Ritz, Daniel](#); [Rock, Lee](#); [Harris, Richard](#); [Falkenstein, Cindy](#)
Cc: [Stempfley, Roberta](#)
Subject: RE: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Date: Wednesday, February 01, 2012 3:21:40 PM

(b) (5)

From: McDermott, Thomas M
Sent: Monday, January 30, 2012 2:50 PM
To: Goode, Brendan; (b) (6) Rock, Lee; Harris, Richard; Falkenstein, Cindy
Cc: Stempfley, Roberta
Subject: FW: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

I'm not sure who is tracking these requirements for CS&C/NCSD.

(b) (5)

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

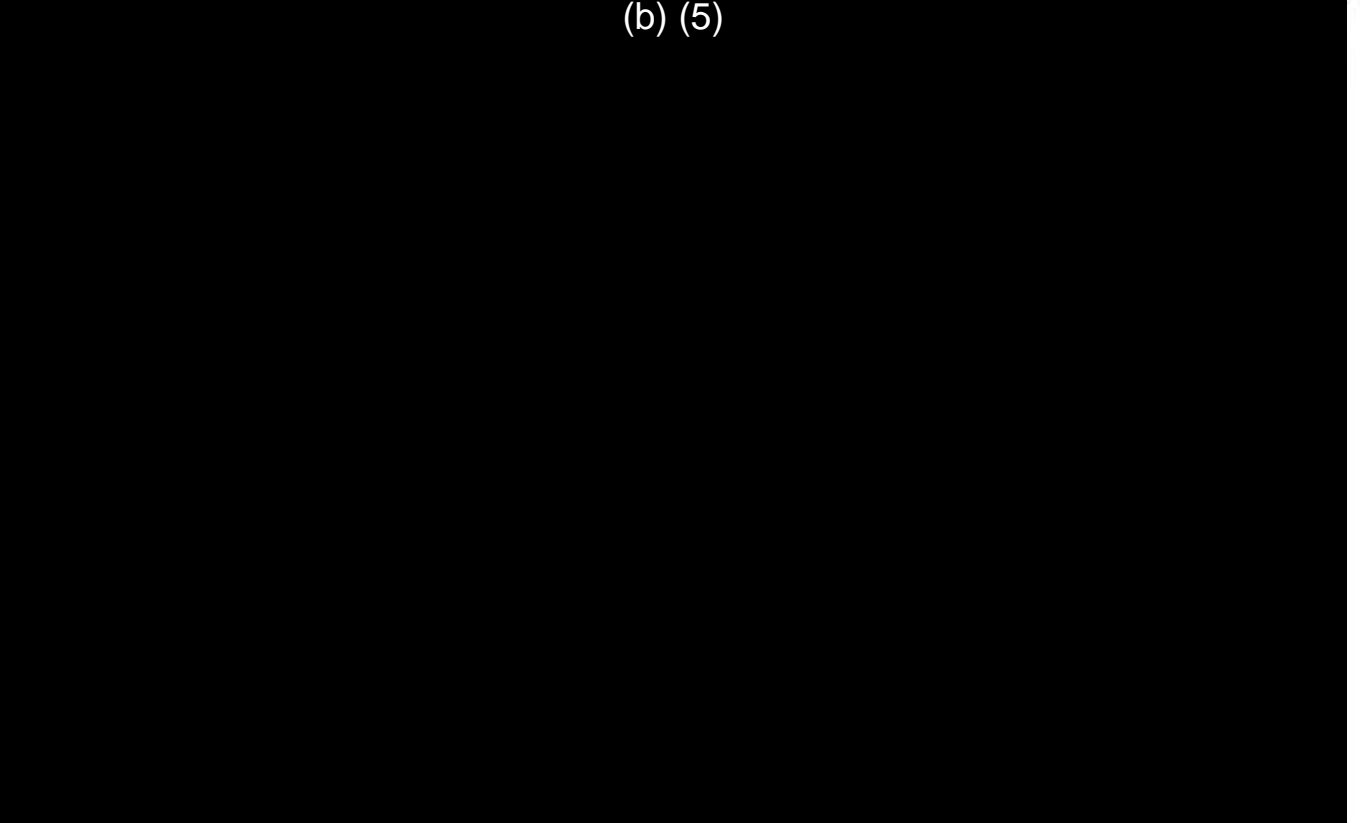
From: (b) (6) (b) (6)
Sent: Monday, January 23, 2012 7:03 PM

To: Schaffer, Gregory; Rosenbach, Eric; (b)(6)-P.L. 86-36; (b) (6) ((b) (6) Stempfley, Bobbie; (b) (6) McConnell, Bruce; (b) (6) McDermott, Thomas M; Goode, Brendan; (b) (6)

Subject: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

All,

(b) (5)



(b) (6)

Director, Cybersecurity
National Security Staff
The White House

(b) (6) v

(b) (6) (direct)

(b) (6) (secure)

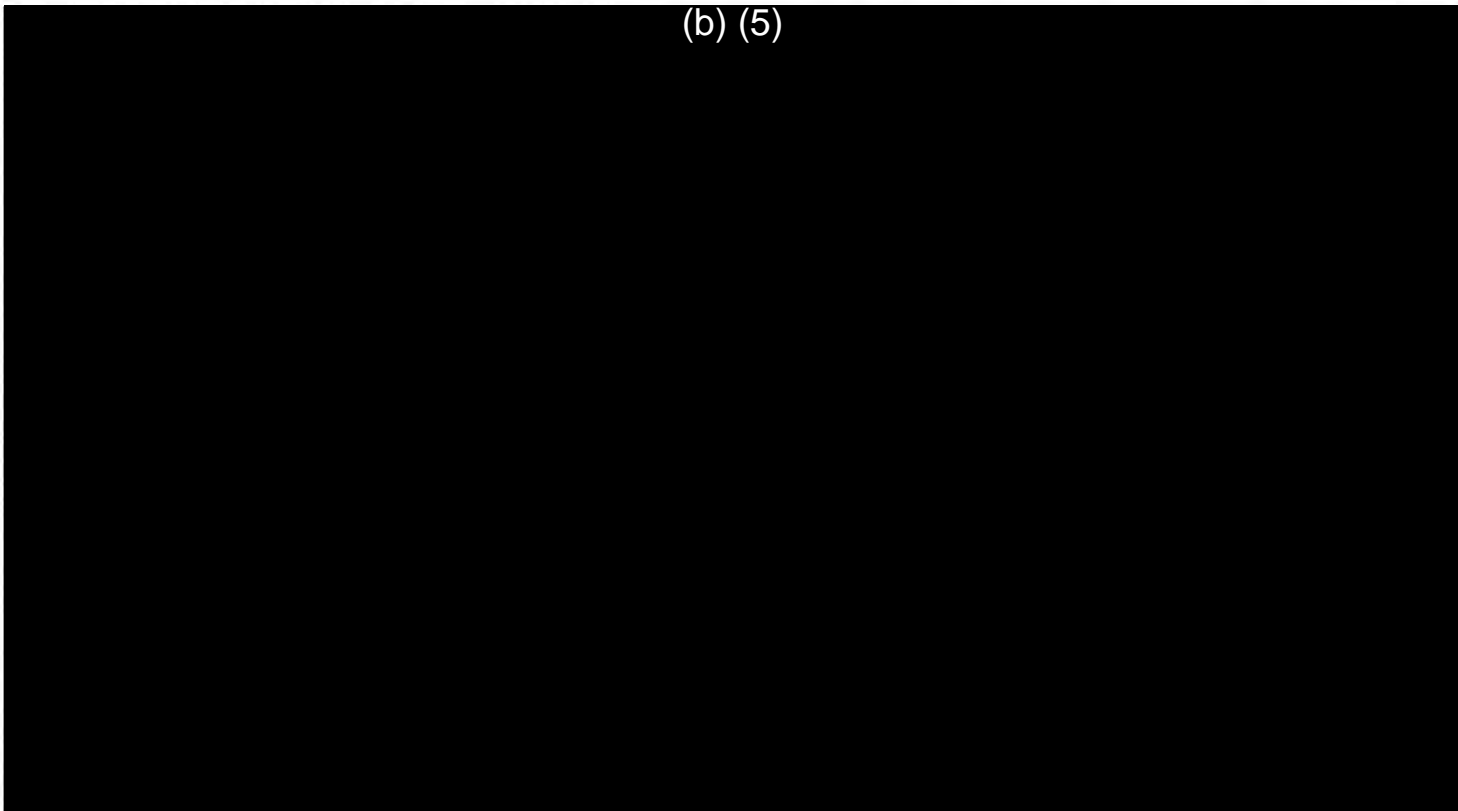
Andrew, Emily

From: Falkenstein, Cindy
Sent: Friday, February 03, 2012 9:55 AM
To: Andrew, Emily; Goode, Brendan; (b) (6) Sand, Peter; (b) (6)
(b) (6) Steiner, Kurt
Cc: Richards, Rebecca; Eberle, Carole; Casapulla, Stephen; (b) (6) Falkenstein, Cindy; (b) (6)
(b) (6)
Subject: UPDATE: NCPS Privacy Compliance WG

All,

Below is an update on the topics normally covered during our workgroup meeting; please let me know if you have any additional updates and we can post to the agenda for our next meeting to be held on Monday, February 13, 2012.

(b) (5)



Cindy Falkenstein

Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: [McDermott, Thomas M](#)
To: (b) (6); [Harris, Richard](#); [Spearman, Verdis](#)
Cc: [Andrew, Emily](#); [Falkenstein, Cindy](#); (b) (6)
Subject: RE: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Date: Friday, February 03, 2012 3:48:16 PM

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: McDermott, Thomas M
Sent: Wednesday, February 01, 2012 3:22 PM
To: McDermott, Thomas M; Goode, Brendan; (b) (6) Rock, Lee; Harris, Richard; Falkenstein, Cindy
Cc: Stempfley, Roberta
Subject: RE: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Following up on this request for DIB Pilot/JCSP policies and procedures by this Friday. Not sure what came out of the meeting between DHS and NSA earlier this week to talk about ConOps/procedures, but hopefully someone is pulling the relevant materials together.

From: McDermott, Thomas M
Sent: Monday, January 30, 2012 2:50 PM
To: Goode, Brendan; (b) (6) Rock, Lee; Harris, Richard; Falkenstein, Cindy
Cc: Stempfley, Roberta
Subject: FW: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

I'm not sure who is tracking these requirements for CS&C/NCSD.

(b) (5)

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs

desk: (b) (6)

blackberry: (b) (6)

(b) (6)

From: (b) (6) (b) (6)

Sent: Monday, January 23, 2012 7:03 PM

To: Schaffer, Gregory; Rosenbach, Eric; (b)(6)-P.L. 86-36; (b) (6) (b) (6) Stempfley, Bobbie; (b) (6) McConnell, Bruce; Skoric, (b) (6) McDermott, Thomas M; Goode, Brendan;

(b) (6) (b) (6)

Subject: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

All,

(b) (5)

Thank you,
Jen

Jennifer Silk
Director, Cybersecurity
National Security Staff
The White House

(b) (6)

(b) (6) (direct)

(b) (6) (secure)

Andrew, Emily

From: McDermott, Thomas M
Sent: Friday, February 03, 2012 5:33 PM
To: (b) (6) Falkenstein, Cindy; Andrew, Emily; (b) (6) Delaney, Laura
Cc: Harris, Richard; Brown, David; (b) (6) Steiner, Kurt; (b) (6) Kinstler, Raymond; Jacobs, Michael; (b) (6) (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

(b) (5)

Does anyone have a sense of who is authorized to make the decision to release these to NSS and/or DOJ today?

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Friday, February 03, 2012 5:08 PM
To: McDermott, Thomas M; Falkenstein, Cindy; Andrew, Emily
Cc: Harris, Richard; Brown, David; (b) (6) Steiner, Kurt; (b) (6) Kinstler, Raymond; Jacobs, Michael; (b) (6) (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

Tom,

Per request of Rick Harris, please find the attached documents categorized below.

Information collection

- SOP 108 – Identifying Sensitive Information
- SOP 110 – PII Handling and Minimization (b) (5)
- SOP 211 – Non-Cyber PII (b) (5)
- (b) (5)

Signature review

- SOP 505 – Creating Initial Signatures from Templates (b) (5)
- SOP 506 – Testing Signatures on Single Sensor (b) (5)
- SOP 507 – Modifying Problem Signatures (b) (5)
- SOP 503 – Testing Signature Templates (b) (5)
- (b) (5)

Data minimization – Data Quality and Integrity

- SOP 108 – Identifying Sensitive Information
- SOP 110 – PII Handling and Minimization
- SOP 121 – Info Sharing with LEI LNOs
- SOP 211 – Non-Cyber PII (b) (5)

- (b) (5)

Security

- SOP 110 – PII Handling and Minimization
- SOP 211 – Non-Cyber PII (b) (5)

Transparency

- Privacy Impact Assessment for the JCSP

Accountability/auditing

- For an example of DHS auditing activity, see the attached Privacy Compliance Review (PCR) for the EINSTEIN Program
- Collateral Information from Early PCR Drafts (b) (5)

Additional references are categorized within the attached “Privacy Oversight Task” document.

If you have any additional questions, please let us know.

Thank you,

(b) (6)

From: McDermott, Thomas M

Sent: Friday, February 03, 2012 4:20 PM

To: Harris, Richard; Falkenstein, Cindy; Andrew, Emily

Cc: Brown, David; (b) (6) Steiner, Kurt; (b) (6) Kinstler, Raymond; Jacobs, Michael;

(b) (6) (b) (6) (b) (6) (b) (6)

Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Are these all currently approved and in place for US-CERT? For example, I’m not sure of the relationship between SOP 108 and 110 both of which appear to discuss PII and minimization.

In addition, we need to indicate which of the SOPs pertain to the different categories highlighted below.

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs

desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Harris, Richard
Sent: Friday, February 03, 2012 4:03 PM
To: McDermott, Thomas M; Falkenstein, Cindy; Andrew, Emily
Cc: Brown, David; (b) (6) Steiner, Kurt; (b) (6) Kinstler, Raymond; Jacobs, Michael;
(b) (6) (b) (6) (b) (6)
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

Tom,

Attached are US-CERT SOPs and other documents that have been collected that address most of the below topics as supporting material for a review of the DIP transition plan:

- Information collection
- Signature review
- Data minimization
- Security
- Transparency
- Accountability/auditing
- Data quality and integrity

I would be happy to submit them to Jennifer or you may do so....

Thanks,
Rick

From: (b) (6)
Sent: Friday, February 03, 2012 3:37 PM
To: Harris, Richard
Cc: (b) (6)
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

FYSA

(b) (6)

From: (b) (6)
Sent: Friday, February 03, 2012 8:36 AM
To: Harris, Richard
Cc: Steiner, Kurt; 'Brown, David'; (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

Rick,

Attached is the combined input from Matt & Kurt. I'm not sure if you have received additional input from people outside of US-CERT that I haven't seen, but I think this is something you should send up instead of it going through ExecSec. (Since it didn't originate there, it might take forever for the response to get to who it needs to go to; which I

think is (b) (6) Bobbie/Schaffer.) Once the response is good to go, I can send up the chain if you would still like me to do so.

Additional input from Kurt to be considered before pushing up the attached documents:

(b) (5)

DHS/NPPD/PIA-021 [National Cyber Security Division Joint Cybersecurity Services Pilot \(JCSP\)](#), January 13, 2012 (PDF, 16 pages – 248 KB).

Please let me know if I can help pull together anything else for this request. Matt/Dave, if Rick is unable to send-up the response before this afternoon; let’s chat and figure out the best way to go forward. I just don’t want this to get lost somewhere.

Due: COB TODAY

Thanks,

(b) (6)

From: Andrew, Emily
Sent: Thursday, February 02, 2012 9:06 AM
To: McDermott, Thomas M; Harris, Richard; Delaney, Laura; Brown, David; (b) (6) (b) (6)
Cc: Falkenstein, Cindy; (b) (6) (b) (6) (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Attached is the document that was provided to NSS. This may have already been circulated by Dan.

From: Falkenstein, Cindy
Sent: Thursday, February 02, 2012 8:52 AM
To: Andrew, Emily
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe Rd (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: McDermott, Thomas M
Sent: Wednesday, February 01, 2012 4:51 PM
To: Harris, Richard; Delaney, Laura; Brown, David; (b) (6) (b) (6)
Cc: (b) (6) (b) (6) (b) (6) Falkenstein, Cindy
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

(b) (5)

That might be a decent starting point for identifying potentially responsive procedures. (Adding Cindy).

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs

desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Harris, Richard
Sent: Wednesday, February 01, 2012 4:15 PM
To: Delaney, Laura; Brown, David; (b) (6) (b) (6)
Cc: (b) (6) (b) (6) (b) (6) McDermott, Thomas M
Subject: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Laura, Dave,

Below is an email tasker that went to the leadership from EOP. It has been bouncing around today without resolution on who will coordinate the task (if I am wrong and NSD is doing this, please let me know). (b) (5)
(b) (5) Jen is looking for a list of references (SOPs, PIAs, etc.) that address each of the topic areas below regarding the Version 10 of the DIB proposal. Request that you designate someone from your staffs to put this collection of references together. I also suspect that we don't have references that cover of all of the topics (like classification guidance), but we should look at the NCPS artifacts as well as E3 related docs to use.....

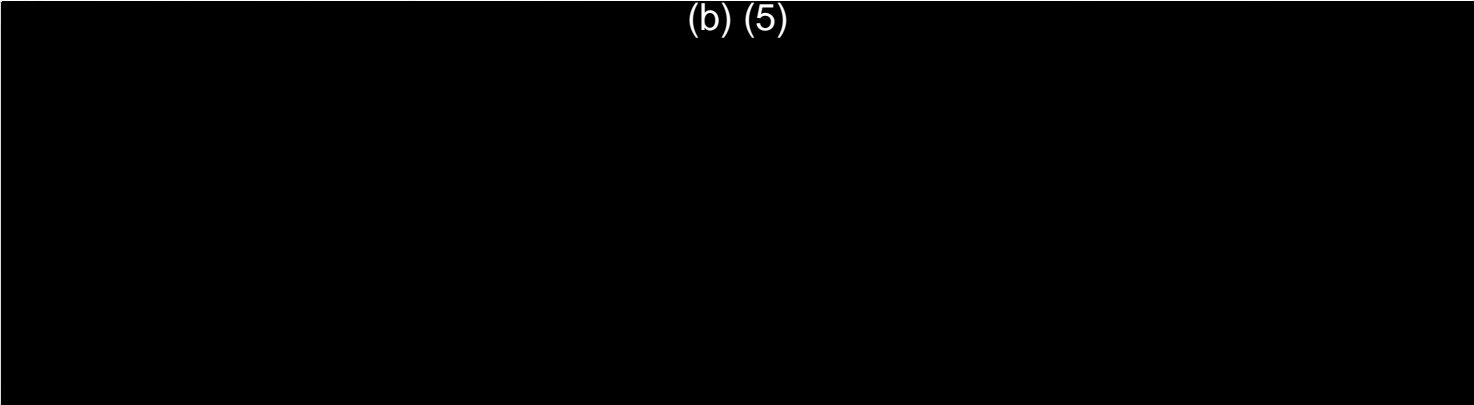
Does this make sense to you?

Thanks,
Rick

From: (b) (6) (b) (6)
Sent: Monday, January 23, 2012 7:03 PM
To: Schaffer, Gregory; Rosenbach, Eric; (b)(6)-P.L. 86-36 (b) (6) (b) (6) Stempfley, Bobbie; (b) (6) McConnell, Bruce; (b) (6) McDermott, Thomas M; Goode, Brendan; (b) (6) (b) (6) (b) (6)
Subject: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

All,

(b) (5)



(b) (5)

Thank you,

(b) (6)

(b) (6)

Director, Cybersecurity
National Security Staff
The White House

(b) (6)

(b) (6) (direct)

(b) (6) (secure)

From: [McDermott, Thomas M](#)
To: (b) (6)
Cc: [Brown, David](#); [Ritz, Daniel](#); [Rock, Lee](#); (b) (6); (b) (6); (b) (6); [Jacobs, Michael](#); [Austin, Mark](#); (b) (6); [Harris, Richard](#); [Andrew, Emily](#); [Falkenstein, Cindy](#)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Date: Tuesday, March 06, 2012 6:16:12 PM
Attachments: [SOP 108 - Identifying Sensitive Information - Final Sept212010.doc](#)
[SOP 110-PII Handling & Minimization.doc](#)
[SOP 121 - Info Sharing with LEI LNOs Final Sept72010.doc](#)
[att moa.pdf](#)
[dhs_CL_moa_signed.pdf](#)

(b) (5)


Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs

desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Tuesday, March 06, 2012 5:38 PM
To: McDermott, Thomas M
Cc: Brown, David; (b) (6) Rock, Lee; (b) (6) (b) (6) (b) (6)
Jacobs, Michael; Austin, Mark; (b) (6) Harris, Richard
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

I was awaiting feedback from the US-CERT stakeholders but since I have not gotten any feedback, I guess I can give you what I have.

(b) (5)



(b) (5)

From: McDermott, Thomas M
Sent: Tuesday, March 06, 2012 5:27 PM
To: (b) (6)
Cc: Brown, David; (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: (b) (6)
Sent: Tuesday, March 06, 2012 9:34 AM
To: McDermott, Thomas M
Cc: Brown, David; (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

(b) (5)

From: McDermott, Thomas M
Sent: Monday, March 05, 2012 5:39 PM
To: Harris, Richard; (b) (6) Goode, Brendan; (b) (6)
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

(b) (5)

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Harris, Richard
Sent: Friday, February 03, 2012 4:03 PM
To: McDermott, Thomas M; Falkenstein, Cindy; Andrew, Emily
Cc: Brown, David; (b) (6) Steiner, Kurt; (b) (6) Kinstler, Raymond; Jacobs, Michael; (b) (6) (b) (6) (b) (6)
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

Tom,

Attached are US-CERT SOPs and other documents that have been collected that address most of the below topics as supporting material for a review of the DIP transition plan:

- Information collection
- Signature review
- Data minimization
- Security
- Transparency
- Accountability/auditing
- Data quality and integrity

I would be happy to submit them to Jennifer or you may do so....

Thanks,
Rick

From: (b) (6)
Sent: Friday, February 03, 2012 3:37 PM
To: Harris, Richard
Cc: (b) (6)
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

FYSA

(b) (6)

From: (b) (6)
Sent: Friday, February 03, 2012 8:36 AM
To: Harris, Richard
Cc: Steiner, Kurt; 'Brown, David'; (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3
Importance: High

Rick,

Attached is the combined input from Matt & Kurt. I'm not sure if you have received additional input from people outside of US-CERT that I haven't seen, but I think this is something you should send up instead of it going through ExecSec. (Since it didn't originate there, it might take forever for the response to get to who it needs to go to; which I think is (b) (6) Bobbie/Schaffer.) Once the response is good to go, I can send up the chain if you would still like me to do so.

Additional input from Kurt to be considered before pushing up the attached documents:

(b) (5)

DHS/NPPD/PIA-021 [National Cyber Security Division Joint Cybersecurity Services Pilot \(JCSP\)](#),
January 13, 2012 (PDF, 16 pages – 248 KB).

Please let me know if I can help pull together anything else for this request. Matt/Dave, if Rick is unable to send-up the response before this afternoon; let's chat and figure out the best way to go forward. I just don't want this to get lost somewhere.

Due: COB TODAY

Thanks,

(b) (6)

From: Andrew, Emily
Sent: Thursday, February 02, 2012 9:06 AM
To: McDermott, Thomas M; Harris, Richard; Delaney, Laura; Brown, David; (b) (6)
(b) (6)
Cc: Falkenstein, Cindy; (b) (6) (b) (6) (b) (6) (b) (6)
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Attached is the document that was provided to NSS. This may have already been circulated by Dan.

From: Falkenstein, Cindy
Sent: Thursday, February 02, 2012 8:52 AM
To: Andrew, Emily
Subject: FW: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Cindy Falkenstein
Senior Privacy Analyst for Cyber Security & Communications (CS&C)
Office of Privacy | National Protection and Programs Directorate | U.S. Department of Homeland Security
1110 N. Glebe (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
(b) (6) | [DHS Privacy Website](#) | [NPPD Privacy Intranet](#)

From: McDermott, Thomas M
Sent: Wednesday, February 01, 2012 4:51 PM
To: Harris, Richard; Delaney, Laura; Brown, David; (b) (6) (b) (6)
Cc: (b) (6) (b) (6) (b) (6) Falkenstein, Cindy
Subject: RE: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

(b) (5)
That might be a decent starting point for identifying potentially responsive procedures. (Adding Cindy).

Thomas M. McDermott
Office of the General Counsel
U.S. Department of Homeland Security,
National Protection and Programs
desk: (b) (6)
blackberry: (b) (6)
(b) (6)

From: Harris, Richard
Sent: Wednesday, February 01, 2012 4:15 PM
To: Delaney, Laura; Brown, David; (b) (6) (b) (6)
Cc: (b) (6) (b) (6) (b) (6) McDermott, Thomas M
Subject: Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

Laura, Dave,

Below is an email tasker that went to the leadership from EOP. It has been bouncing around today without resolution on who will coordinate the task (if I am wrong and NSD is doing this, please let me know). (b) (5)

Jen is looking for a list of references (SOPs, PIAs, etc.) that address each of the topic areas below regarding the Version 10 of the DIB proposal. Request that you designate someone from your staffs to put this collection of references together. I also suspect that we don't have references that cover of all of the topics (like classification guidance), but we should look at the NCPS artifacts as well as E3 related docs to use.....

Does this make sense to you?

Thanks,
Rick

From: (b) (6) (b) (6)
Sent: Monday, January 23, 2012 7:03 PM
To: Schaffer, Gregory; Rosenbach, Eric; (b)(6)-P.L. 86-36; (b) (6) (b) (6) Stempfley, Bobbie; (b) (6) McConnell, Bruce; (b) (6) McDermott, Thomas M; Goode, Brendan; (b) (6) (b) (6)
Subject: For Action: Information handling policies and procedure references for DIB Proposal, due COB Feb 3

All,

(b) (5)

Thank you,

(b) (6)

(b) (6)
Director, Cybersecurity
National Security Staff
The White House
(b) (6)
(b) (6) (direct)
(b) (6) (secure)

From: Andrew, Emily
To: (b) (6)
Cc: Lockett, Vania
Subject: FW: Meeting to discuss Defense Industrial Base initiatives -- 5/22 at 3:00 p.m.
Date: Friday, May 18, 2012 4:36:53 PM

FYI – Brendan will be attending this meeting with Mary Ellen next week.

Emily

From: Callahan, Mary Ellen
Sent: Friday, May 18, 2012 12:12 PM
To: Goode, Brendan; Andrew, Emily; McDermott, Thomas M
Subject: FW: Meeting to discuss Defense Industrial Base initiatives -- 5/22 at 3:00 p.m.

FYI. Brendan, do you want me to confirm for you? mec

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)
Fax: (b) (6)
E-mail: (b) (6)
Website: www.dhs.gov/privacy

From: (b) (6); (b) (6)
Sent: Friday, May 18, 2012 12:08 PM
To: (b) (6); 'Rosenbach, Eric B SES OSD POLICY'; (b)(6)-P.L. 86-36; (b) (6)
 (b) (6) McConnell, Bruce; 'Stempfley, Roberta (b) (6)
 'Rosenbach, Eric B SES OSD POLICY'; 'Schleien, Steven, SES, OSD-POLICY'; (b) (6)
 (b) (6); (b) (6); (b) (6) Callahan, Mary Ellen
Cc: (b) (6); (b) (6)
Subject: FW: Meeting to discuss Defense Industrial Base initiatives -- 5/22 at 3:00 p.m.

All –

To follow up on our prep call, I’m forwarding the invitation that went out to representatives of privacy and civil liberties advocacy groups. As a reminder, the meeting will be in (b) (6) of the White House Conference Center, starting at 3:00 on Tuesday, May 22. Directions are in the body of the email I’m forwarding.

The attendees and represented organizations are:

- ACLU: Michelle Richardson, legislative counsel, <http://www.aclu.org/blog/author/michelle-richardson>
- Center for Democracy & Technology: Greg Nojeim, senior counsel and Director of Project

on Freedom, Security, and Technology, <https://www.cdt.org/personnel/greg-nojeim>; and Kendall Burman, senior national security fellow, <https://www.cdt.org/personnel/kendall-burman>

- Constitution Project: Sharon Bradford Franklin, senior counsel, Rule of Law project, <http://www.constitutionproject.org/staff/bradfordfranklin.php>
- Electronic Frontier Foundation: Lee Tien, senior staff attorney (invited but not attending), <https://www.eff.org/about/staff>
- Electronic Privacy Information Center (EPIC): Lillie Coney, Associate Director, http://epic.org/epic/staff_and_board.html

Based on this morning's call, this is the list we have for USG participants:

- DHS: Mary Ellen Callahan and one policy/program rep (DHS will confirm)
- DOD: (b) (6) (DOD will confirm)
- NSA: (b)(6)-P.L. 86-36

Please keep in mind the overall group size and try to limit agency participation to 1-2 participants.

Finally, we request from DOD final PA materials and a link to your PIA by COB today if possible. (Thanks, Mary Ellen, for sending the DHS PIA.)

Please let me know if you have any questions.

Thank you,

(b) (6)

From: (b) (6)

Sent: Wednesday, May 16, 2012 2:58 PM

To: Richardson, Michelle (b) (6)

Cc: (b) (6) (b) (6) (b) (6)

Subject: Meeting to discuss Defense Industrial Base initiatives -- 5/22 at 3:00 p.m.

The Department of Defense (DoD), in partnership with the Department of Homeland Security (DHS), announced two important efforts to address Defense Industrial Base cybersecurity concerns on Friday, May 11. These two initiatives involve a novel set of policy issues, so we are convening a meeting with DoD and DHS officials to describe the details of these cybersecurity efforts to you, as well as the Administration's ongoing efforts to address privacy and civil liberties concerns relating to cybersecurity in regards to these efforts.

Please let me know if you will be able to join us on **Tuesday, May 22, at 3:00 p.m.** in the White House Conference Center, Wilson Room.

Directions to the White House Conference Center

The White House Conference Center is at 726 Jackson PI NW, Washington, DC, on the east side of Lafayette square: <http://bit.ly/ktCb15>. You will need to show a photo ID to enter the Conference

Center, but you do not need to submit any information in advance. If you have any problems, please contact our administrative assistant (b) (6), at (b) (6) or by email at (b) (6)

Best regards,

(b) (6)

(b) (6)

Director for Privacy and Civil Liberties

National Security Staff

(b) (6)

(b) (6) (direct)

Andrew, Emily

From: Sand, Peter
Sent: Thursday, May 26, 2011 10:01 AM
To: Callahan, Mary Ellen; Andrew, Emily; Rebecca J. Richards (b) (6)
Cc: John W. Kropf (b) (6) (b) (6) Leckey, Eric
Subject: [Cyber] Status on DIB Pilot, DOD's PIA

Looks like PIA (b) (5)

(b) (5)