From: Andrew, Emily
To: Lockett, Vania; Falkenstein, Cindy
Subject: FW: FYI DIB Pilot PIA published
Date: Wednesday, August 03, 2011 2:52:25 PM
Attachments: DIB CS-IA PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

(b) (5)

Stay tuned.

From: Sand, Peter
Sent: Wednesday, August 03, 2011 2:44 PM
To: Callahan, Mary Ellen; John W. Kropf (b) (6) Andrew, Emily; Brown, Michael A. RADM; (b) (6); (b) (6) (b) (6) Delaney, David; McNeely, James; McDermott, Thomas M
Subject: FYI DIB Pilot PIA published

Looks like it published June 30th...

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

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
To: Falkenstein, Cindy
Subject: RE: DoD to Expand DIB Cyber program
Date: Monday, August 22, 2011 7:48:55 AM

Cindy – can you add: [redacted] for today?

From: Sand, Peter
Sent: Friday, August 19, 2011 12:08 PM
To: Andrew, Emily
Cc: Callahan, Mary Ellen; Hunt, Ken; Foster, Helen; Kropf, John
Subject: RE: DoD to Expand DIB Cyber program

Emily,
Check it: "The program is being expanded to the entire DIB, as well as other key areas of critical infrastructure"

[redacted]

[redacted]
.. .seems like exactly the same thing...

DoD to expand pilot program that shares classified threat intelligence with industry

18 August 2011

The Department of Defense (DoD) is expanding a pilot program that shares classified cybersecurity information with a number of defense contractors to the entire industry, William Lynn, deputy secretary of defense, told a defense industry conference in Baltimore this week.

Under the Defense Industrial Base (DIB) Cyber Pilot program, which was launched in May in partnership with the Department of Homeland Security, the DoD shared classified threat intelligence with 20 defense contractors and their commercial internet service providers, as well as information on how to employ the intelligence in network defense.

Lynn told the conference that the pilot program had already stopped hundreds of attempted network intrusions.

"The government has deep awareness of certain cyber threats. We have what some have termed a 'special sauce' of malicious code signatures gathered from various intelligence efforts. Loading these signatures onto existing systems dramatically increases the effectiveness of cybersecurity", Lynn explained.

The program is being expanded to the entire DIB, as well as other key areas of critical infrastructure. Lynn emphasized that the program is voluntary, and that the government is not monitoring, intercepting, or storing any private sector communications as part of the effort.

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

From: Kropf, John
Sent: Friday, August 19, 2011 11:52 AM
To: Sand, Peter; Foster, Helen; Hunt, Ken
Cc: Callahan, Mary Ellen
Subject: DoD to Expand DIB Cyber program

DoD To Expand Pilot Program That Shares Classified Threat Intelligence With Industry: The Department of Defense (DoD) is expanding a pilot program that shares classified cybersecurity information with a number of defense contractors to the entire industry, William Lynn, deputy secretary of defense, told a defense industry conference in Baltimore this week. Under the Defense Industrial Base (DIB) Cyber Pilot program, which was launched in May in partnership with the Department of Homeland Security, the DoD shared classified threat intelligence with 20 defense contractors and their commercial internet service providers, as well as information on how to employ the intelligence in network defense. [HSEC-1.9; Date: 18 August 2011; Source: http://www.infosecurity-us.com/view/20195/dod-to-expand-pilot-program-that-shares-classified-threat-intelligence-with-industry/]

John W. Kropf
Deputy Chief Privacy Officer
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)
(b) (6)

From: Andrew, Emily
To: Steiner, Kurt
Cc: Falkenstein, Cindy
Subject: RE: DoD to Expand DIB Cyber program
Date: Tuesday, August 23, 2011 8:39:13 AM

[redacted] (b) (5)

From: Steiner, Kurt
Sent: Tuesday, August 23, 2011 8:34 AM
To: Andrew, Emily
Cc: Falkenstein, Cindy
Subject: RE: DoD to Expand DIB Cyber program

DIB Pilot Expansion – [redacted] (b) (5)
[redacted] (b) (5)

Regards,

Kurt

From: Andrew, Emily
Sent: Tuesday, August 23, 2011 7:21 AM
To: Steiner, Kurt
Subject: FW: DoD to Expand DIB Cyber program

Sorry – I thought Cindy was sending this on.

Emily

From: Andrew, Emily
Sent: Monday, August 22, 2011 2:29 PM
To: Falkenstein, Cindy
Subject: FW: DoD to Expand DIB Cyber program

Here's the article below.

DoD to expand pilot program that shares classified threat intelligence with industry

18 August 2011

The Department of Defense (DoD) is expanding a pilot program that shares classified cybersecurity information with a number of defense contractors to the entire industry, William Lynn, deputy secretary of defense, told a defense industry conference in Baltimore this week.

Under the Defense Industrial Base (DIB) Cyber Pilot program, which was launched in May in partnership with the

Department of Homeland Security, the DoD shared classified threat intelligence with 20 defense contractors and their commercial internet service providers, as well as information on how to employ the intelligence in network defense.

Lynn told the conference that the pilot program had already stopped hundreds of attempted network intrusions.

"The government has deep awareness of certain cyber threats. We have what some have termed a 'special sauce' of malicious code signatures gathered from various intelligence efforts. Loading these signatures onto existing systems dramatically increases the effectiveness of cybersecurity", Lynn explained.

The program is being expanded to the entire DIB, as well as other key areas of critical infrastructure. Lynn emphasized that the program is voluntary, and that the government is not monitoring, intercepting, or storing any private sector communications as part of the effort.

DoD To Expand Pilot Program That Shares Classified Threat Intelligence With Industry: The Department of Defense (DoD) is expanding a pilot program that shares classified cybersecurity information with a number of defense contractors to the entire industry, William Lynn, deputy secretary of defense, told a defense industry conference in Baltimore this week. Under the Defense Industrial Base (DIB) Cyber Pilot program, which was launched in May in partnership with the Department of Homeland Security, the DoD shared classified threat intelligence with 20 defense contractors and their commercial internet service providers, as well as information on how to employ the intelligence in network defense. [HSEC-1.9; Date: 18 August 2011; Source: http://www.infosecurity-us.com/view/20195/dod-to-expand-pilot-program-that-shares-classified-threat-intelligence-with-industry/]

From: Andrew, Emily
To: Falkenstein, Cindy; (b) (6) Steiner, Kurt; Richards, Rebecca; Sand, Peter; (b) (6) Leckey, Eric; (b) (6)
Cc: Andrew, Emily; Casapulla, Stephen; Goode, Brendan; Eberle, Carole
Subject: RE: NCPS Privacy Compliance Workgroup Meeting 08222011
Date: Wednesday, August 24, 2011 11:27:45 AM
Attachments: NCSD IA Block 3 Overview (tkelly).ppt
NCPS Privacy Compliance Workgroup Minutes 08222011.docx

All – attached are the meeting minutes from Monday.

The next meeting is scheduled for Monday Sept 5th which is Labor Day. Since we have a number of deliverables coming up rather quickly, we'd like to propose having the meeting **on Tuesday Sept 6th at 2pm**.

Please let us know if this works and if not, please propose alternative dates and times.

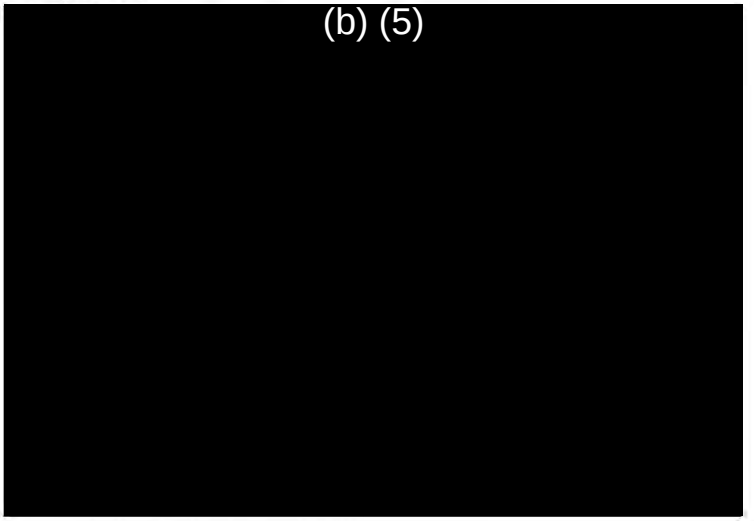
Thanks
Emily

From: Falkenstein, Cindy
Sent: Monday, August 22, 2011 8:46 AM
To: Andrew, Emily; Richards, Rebecca; (b) (6) Leckey, Eric; Sand, Peter; (b) (6) Falkenstein, Cindy
Cc: Casapulla, Stephen; Goode, Brendan; Eberle, Carole; (b) (6) Steiner, Kurt
Subject: NCPS Privacy Compliance Workgroup Meeting 08222011

Below is the agenda for Today's NCPS Privacy Compliance Workgroup call. If for some reason you can't make the call – please send your updates. For your convenience I am attaching the minutes from the last call (August 8, 2011).

Team updates:

(b) (5)



(b) (5)

Cindy V. Falkenstein
Senior Privacy Analyst
National Protection and Programs Directorate /
U.S. Department of Homeland Security
(b) (6)
Tel: (b) (6)
Cell: (b) (6)

Andrew, Emily

From: Andrew, Emily
Sent: Thursday, November 03, 2011 8:48 AM
To: Goode, Brendan; Dean, Nicole M
Cc: Sand, Peter
Subject: FW: DHS/DoD Coordination

Brendan/ Nicole – See message below from a gentleman from Carnegie Mellon looking for info on the DIB Pilot evaluation. Looks like [redacted (b) (5)]

Emily

From: Sand, Peter
Sent: Thursday, November 03, 2011 7:23 AM
To: Andrew, Emily
Cc: John W. Kropf [redacted (b) (6)]
Subject: FW: DHS/DoD Coordination

Emily

Before I respond to this guy, [redacted (b) (5)] [redacted (b) (5)]

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! [redacted (b) (6)].

From: Travis Breaux [redacted (b) (6)]
Sent: Wednesday, November 02, 2011 12:00 PM
To: [redacted (b) (6)]
Cc: [redacted (b) (6)]
Subject: DHS/DoD Coordination

Hi Peter,

John Kropf gave me your name and recommended that I get in touch with you. I'm conducting the independent privacy evaluation of the DoD DIB Cyber Pilot program with an eye to the future (see link below). I'm interested in speaking to someone in the DHS Privacy Office who could help answer a few questions and provide their insight.

I will try calling your office this afternoon, but if there is a good time chat tomorrow or Friday morning, I can call at a scheduled time that works better for you.

http://www.gsnmagazine.com/node/24798

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Andrew, Emily
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6) (b) (6)
Subject: Re: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)
Date: Tuesday, November 22, 2011 4:04:59 PM

Not sure, we need a briefing. (b) (6) mentions us taking over immediately. I'll see what I can find out.

From: Sand, Peter
Sent: Tuesday, November 22, 2011 04:02 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6) (b) (6) (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Emily,

(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: Andrew, Emily
Sent: Tuesday, November 22, 2011 3:59 PM
To: (b) (6) Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6) (b) (6)
Subject: Re: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Yes, (b) (5)
(b) (5)

Can you get that to us ASAP? We are available to meet next week or we can use our work group time on Monday to discuss.

Emily

From: (b) (6)
Sent: Tuesday, November 22, 2011 03:27 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan
Subject: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Emily/Cindy –

(b) (5)

Are either of you free early next week to discuss next steps and what information you need from us to get this evaluation/effort started?

Thanks,
(b) (6)

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

From: Andrew, Emily
To: (b) (6); Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)
Date: Wednesday, November 23, 2011 2:39:40 PM

Thanks – please provide as much detail as possible so we can determine next steps.

From: (b) (6)
Sent: Wednesday, November 23, 2011 2:38 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

I'm shooting to have the PTA to you next week.

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

From: Andrew, Emily
Sent: Wednesday, November 23, 2011 2:28 PM
To: (b) (6), Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

(b) (6),

Unfortunately (b) (5). How soon can you get me a PTA?

Emily

From: (b) (6)
Sent: Wednesday, November 23, 2011 2:22 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Emily –

Below is a brief summary. (b) (5)

(b) (5)

Thanks,
(b) (6)

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

From: Andrew, Emily
Sent: Tuesday, November 22, 2011 4:06 PM
To: (b) (6); Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6)
Subject: Re: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

(b) (5)

From: (b) (6)
Sent: Tuesday, November 22, 2011 04:03 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6); (b) (6); (b) (6)
Subject: RE: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

I have the PTA template and we will start drafting this week/early next week.

Using our work group time on Monday works for me, but Brendan will be in Acquisition training all week and may not be available at that time.

(b) (6)
DHS/NCSD/NSD
(b) (6)
(b) (6) (Telework Location)

(b) (6) (Ballston Office)
(b) (6) (BlackBerry)

From: Andrew, Emily
Sent: Tuesday, November 22, 2011 3:59 PM
To: (b) (6) Falkenstein, Cindy
Cc: Goode, Brendan; Sand, Peter; (b) (6) (b) (6)
Subject: Re: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Yes, (b) (5)

Can you get that to us ASAP? We are available to meet next week or we can use our work group time on Monday to discuss.

Emily

From: (b) (6)
Sent: Tuesday, November 22, 2011 03:27 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: Goode, Brendan
Subject: Potential Privacy Engagement: Joint Cybersecurity Services Pilot (JCSP)

Emily/Cindy –

(b) (5)

Are either of you free early next week to discuss next steps and what information you need from us to get this evaluation/effort started?

Thanks,
(b) (6)

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

From: Sand, Peter
To: Andrew, Emily; Richards, Rebecca; (b) (6) ; Falkenstein, Cindy
Cc: Callahan, Mary Ellen; Lockett, Vania
Subject: RE: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)
Date: Monday, November 28, 2011 11:09:52 AM

Emily,

(can't copy/paste from .pdf)

(b) (5)

Pete

From: Andrew, Emily
Sent: Mon 11/28/2011 10:58 AM
To: Sand, Peter; Richards, Rebecca; (b) (6) ; Falkenstein, Cindy
Cc: Callahan, Mary Ellen; Lockett, Vania
Subject: FW: [SOC] White House Actions Tasking - NSS - Paper DC on DIB Pilot Extension - (Due 11.10.11 0900)

Attached is some additional info on the DIB pilot. I did speak with our CIO this morning and it looks like it's going to be a heavy lift for them to get this done within 60 days. Hopefully we will learn more today during our workgroup call.

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)

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 (b) (5) 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 (b) (5). 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

(b) (5)

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	Requirement: 1) ***Deputy Secretary*-level comments/approval** on the paper in a *consolidated* and *adjudicated* comment matrix. (***Matrix must 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	COORDINATING COMPONENTS: Please work with NPPD as soon as possible. NPPD will lead and submit the final document to DHS Exec Sec. OGC Coordination: 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, 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)
Office of the Executive Secretary
Office of the Secretary
Department of Homeland Security
(b) (6)

Andrew, Emily

From: Falkenstein, Cindy
Sent: Tuesday, November 29, 2011 6:00 PM
To: Andrew, Emily
Subject: RE: JCSP Transition Activities

In brief, the topics of discussion were:

(b) (5)

[redacted]

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, November 29, 2011 5:16 PM
To: Falkenstein, Cindy
Subject: Re: JCSP Transition Activities

Thanks

From: Falkenstein, Cindy
Sent: Tuesday, November 29, 2011 05:01 PM
To: Andrew, Emily
Subject: RE: JCSP Transition Activities

Yes, was just dialing in.

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, November 29, 2011 5:01 PM
To: Falkenstein, Cindy
Subject: FW: JCSP Transition Activities

You're attending the calls right?

From: (b) (6)
Sent: Tuesday, November 29, 2011 4:48 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Please find an updated draft agenda for the CIO/CISO meeting attached.

Thanks,

(b) (6)

<< File: CIO-CISO JCSP Meeting Agenda_Draft_11292011.doc >>

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

From: (b) (6)
Sent: Tuesday, November 29, 2011 12:06 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Attached is a draft agenda for the CIO/CISO meeting in mid-December. Please be ready to discuss at this evening's call. If you have any additions/modifications, please send them along and I will try to incorporate before our call at 5:00 << File: CIO-CISO JCSP Meeting Agenda_Draft_11292011.doc >> .

(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, November 29, 2011 10:20 AM
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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Attached is the latest activity tracker, which reflects status on actions from last night's call.

Carolyn

<< File: JCSS_Action Tracker_11212011.xls >>

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

-----Original Appointment-----
From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Monday, November 21, 2011 1:53 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
Subject: JCSP Transition Activities
When: Occurs every weekday effective 11/28/2011 until 2/29/2012 from 5:00 PM to 6:00 PM (GMT-05:00) Eastern Time

00156
(US & Canada).
Where: Phoncon (b) (6) #(b) (6)

Andrew, Emily

From: Goode, Brendan
Sent: Wednesday, November 30, 2011 8:15 PM
To: (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

Attached is a very rough draft of the voice track for the CIO/CISO briefing. The purpose of this document is to lay out the logical flow of the briefing and to act as the basis for the talking points for Greg.

Based on the general flow of the voice track (and the talking points), we'll begin pulling together a skeleton of the briefing tonight and tomorrow.

Please let me know if you have comments so that we can incorporate it in this talking points and the briefing.

Thanks,
Brendan

Voice Track for the CIO-CISO B...

From: (b) (6)
Sent: Wednesday, November 30, 2011 5:31 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Updated tracker with tonight's status is attached.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

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

From: (b) (6)
Sent: Wednesday, November 30, 2011 12:20 PM
To: Dean, Nicole M; McDermott, Thomas M; (b) (6) Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos;

00158
Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6) (b) (6) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan
Subject: RE: JCSP Transition Activities

All,

Attached is the tracker as of last night's meeting.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

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

-----Original Appointment-----
From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Monday, November 21, 2011 1:53 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
Subject: JCSP Transition Activities
When: Occurs every weekday effective 11/28/2011 until 2/29/2012 from 5:00 PM to 6:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: Phoncon (b) (6) #(b) (6)

Andrew, Emily

From: (b) (6)
Sent: Tuesday, November 29, 2011 4:48 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Please find an updated draft agenda for the CIO/CISO meeting attached.

Thanks,
(b) (6)

CIO-CISO JCSP Meeting Agenda_D..

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

From: (b) (6)
Sent: Tuesday, November 29, 2011 12:06 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Attached is a draft agenda for the CIO/CISO meeting in mid-December. Please be ready to discuss at this evening's call. If you have any additions/modifications, please send them along and I will try to incorporate before our call at 5:00 << File: CIO-CISO JCSP Meeting Agenda_Draft_11292011.doc >> .

(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, November 29, 2011 10:20 AM
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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Attached is the latest activity tracker, which reflects status on actions from last night's call.

Carolyn

<< File: JCSS_Action Tracker_11212011.xls >>

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

-----Original Appointment-----
From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Monday, November 21, 2011 1:53 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
Subject: JCSP Transition Activities
When: Occurs every weekday effective 11/28/2011 until 2/29/2012 from 5:00 PM to 6:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: Phoncon (b) (6) #(b) (6)

00161

Andrew, Emily

From: Dean, Nicole M
Sent: Thursday, December 01, 2011 10:24 AM
To: Goode, Brendan; (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

Voice Track for the CIO-CISO B...

With my comments

From: Goode, Brendan
Sent: Wednesday, November 30, 2011 8:15 PM
To: (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

Attached is a very rough draft of the voice track for the CIO/CISO briefing. The purpose of this document is to lay out the logical flow of the briefing and to act as the basis for the talking points for Greg.

Based on the general flow of the voice track (and the talking points), we'll begin pulling together a skeleton of the briefing tonight and tomorrow.

Please let me know if you have comments so that we can incorporate it in this talking points and the briefing.

Thanks,
Brendan

<< File: Voice Track for the CIO-CISO Briefing.doc >>

From: (b) (6)
Sent: Wednesday, November 30, 2011 5:31 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Updated tracker with tonight's status is attached.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

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

From: (b) (6)
Sent: Wednesday, November 30, 2011 12:20 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan
Subject: RE: JCSP Transition Activities

All,

Attached is the tracker as of last night's meeting.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

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

-----Original Appointment-----
From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Monday, November 21, 2011 1:53 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
Subject: JCSP Transition Activities
When: Occurs every weekday effective 11/28/2011 until 2/29/2012 from 5:00 PM to 6:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: Phoncon (b) (6) # (b) (6)

Andrew, Emily

From: Dean, Nicole M
Sent: Thursday, December 01, 2011 12:51 PM
To: McDermott, Thomas M; Goode, Brendan; (b) (6) (b) (6); Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6) (b) (6) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities - banner meeting

Thanks Tom. (b) (5). On the call tonight we can discuss our thoughts for agenda items and hopefully we'll have their by then also.

From: McDermott, Thomas M
Sent: Thursday, December 01, 2011 10:16 AM
To: Dean, Nicole M; Goode, Brendan; (b) (6) (b) (6) Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6) (b) (6) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities - banner meeting

(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: Dean, Nicole M
Sent: Thursday, December 01, 2011 9:54 AM
To: Goode, Brendan; (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: JCSP Transition Activities - banner meeting

Tom,

(b) (5)

Nicole

From: Andrew, Emily
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines
Date: Friday, December 02, 2011 10:07:57 AM

Cindy – just saw your earlier message regarding Kurt. (b) (5) .

From: Sand, Peter
Sent: Friday, December 02, 2011 10:03 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Then I'll send MEC this language and note that we are also sending it through NPPD for their clearance.

I didn't mention any specific SOPs – I'm sure he will ask for them as a follow up.

I recall there once was a separate SOP that specifically laid out the development of templates and signatures. I pulled the language I used from SOP 108 and 445.

If he does ask for the actual SOPs, I am going to defer to NPPD because they are NPPD docs.

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: Andrew, Emily
Sent: Friday, December 02, 2011 9:58 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)

Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

(b) (5)

From: Sand, Peter
Sent: Friday, December 02, 2011 9:25 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

(b) (5)

I am also sending to MEC for review.

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: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 1:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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: Travis Breaux (b) (6)
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Falkenstein, Cindy
To: Steiner, Kurt
Subject: FW: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines
Date: Friday, December 02, 2011 10:25:00 AM
Attachments: SOP 108 - Identifying Sensitive Information - Final Sept212010.docx
SOP 445 - Tier 1 PCAP Collection - Final Aug22010.doc

Hi,

(b) (5)

Can you or Chris follow up with Tom or Brendan? They were both at the meeting yesterday and may have some more insight on what was discussed.

(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: Sand, Peter
Sent: Friday, December 02, 2011 10:03 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Then I'll send MEC this language and note that we are also sending it through NPPD for their clearance.

I didn't mention any specific SOPs – I'm sure he will ask for them as a follow up.

I recall there once was a separate SOP that specifically laid out the development of templates and signatures. I pulled the language I used from SOP 108 and 445.

If he does ask for the actual SOPs, I am going to defer to NPPD because they are NPPD docs.

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: Andrew, Emily
Sent: Friday, December 02, 2011 9:58 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

(b) (5)

From: Sand, Peter
Sent: Friday, December 02, 2011 9:25 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

(b) (5)

(b) (5)

I am also sending to MEC for review.

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: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 1:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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: Travis Breaux (b) (6)
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Goode, Brendan
To: Dean, Nicole M; (b) (6); McDermott, Thomas M; Taran, (b) (6); Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6); (b) (6); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities
Date: Friday, December 02, 2011 4:37:37 PM

Effective today or next week?

From: Dean, Nicole M
Sent: Friday, December 02, 2011 4:01 PM
To: (b) (6); Goode, Brendan; 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); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

(b) (5)

Nicole

From: (b) (6)
Sent: Thursday, December 01, 2011 5:40 PM
To: Dean, Nicole M; Goode, Brendan; 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); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

The updated Activity Tracker is attached. I won't be able to call into the meeting tomorrow evening, so please forward any updates that need to be included by email so that I can update accordingly for Monday's call.

Thanks,

(b) (6)

<< File: JCSS_Action Tracker_11212011.xls >>

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

From: Dean, Nicole M
Sent: Thursday, December 01, 2011 10:24 AM
To: Goode, Brendan; (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

With my comments << File: Voice Track for the CIO-CISO Briefing nmd.doc >>

From: Goode, Brendan
Sent: Wednesday, November 30, 2011 8:15 PM
To: (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

Attached is a very rough draft of the voice track for the CIO/CISO briefing. The purpose of this document is to lay out the logical flow of the briefing and to act as the basis for the talking points for Greg.

Based on the general flow of the voice track (and the talking points), we'll begin pulling together a skeleton of the briefing tonight and tomorrow.

Please let me know if you have comments so that we can incorporate it in this talking points and the briefing.

Thanks,

Brendan

<< File: Voice Track for the CIO-CISO Briefing.doc >>

From: (b) (6)
Sent: Wednesday, November 30, 2011 5:31 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan; Falkenstein, Cindy; Andrew, Emily
Subject: RE: JCSP Transition Activities

All,

Updated tracker with tonight's status is attached.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

From: (b) (6)
Sent: Wednesday, November 30, 2011 12:20 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Goode, Brendan
Subject: RE: JCSP Transition Activities

All,

Attached is the tracker as of last night's meeting.

(b) (6) << File: JCSS_Action Tracker_11212011.xls >>

(b) (6)

DHS/NCSD/NSD

(b) (6)

(b) (6) (Telework Location)

(b) (6) (Ballston Office)

(b) (6) (BlackBerry)

-----Original Appointment-----
From: (b) (6) **On Behalf Of** Dean, Nicole M
Sent: Monday, November 21, 2011 1:53 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
Subject: JCSP Transition Activities
When: Occurs every weekday effective 11/28/2011 until 2/29/2012 from 5:00 PM to 6:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: Phoncon (b) (6) #(b) (6)

From: Dean, Nicole M
To: [redacted]; Goode, Brendan; McDermott, Thomas M; [redacted] Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; [redacted] Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: DIB Pilot Evaluation Report
Date: Friday, December 02, 2011 4:39:35 PM
Attachments: DIB Pilot Evaluation Report 113011_v1_NO SECTIONS 4 AND 5_DRAFT-FINAL.PDF

All,

Here is the DIB pilot final report.

Andrew, Emily

From: Falkenstein, Cindy
Sent: Friday, December 02, 2011 6:13 PM
To: Andrew, Emily
Subject: 12/02/11 JCSP telecom

Recap of (b) (5)

- very productive, focus on short term goals

(b) (5)

- finalize interagency talking points: plan to complete by Wed. In prep for CIO/CISO mtg. And in prep for DIB mtg next Friday: Bobbie will cover CIO/CISO mtg. (b) (5)

- Vision: (b) (5)

(b) (5)

- Final notes:

(b) (5)

Cindy V. Falkenstein
Senior Privacy Analyst
U.S. Dept. Of Homeland Security
(b) (6)
Tel; (b) (6)
Cell: (b) (6)

From: Falkenstein, Cindy
To: Andrew, Emily
Subject: Re: DIB Pilot Evaluation Report
Date: Friday, December 02, 2011 5:05:11 PM

Sure, getting a recap on the AM Mtg.
now
Cindy V. Falkenstein
Senior Privacy Analyst
U.S. Dept. Of Homeland Security
(b) (6)
Tel; (b) (6)
Cell: (b) (6)

From: Andrew, Emily
Sent: Friday, December 02, 2011 05:03 PM
To: Sand, Peter; (b) (6)
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: Re: DIB Pilot Evaluation Report

Cindy,

If you have an opportunity on the call tonight can you ask if this is the final? If not, can you let Tom and Brendan know we need feedback?

Thanks

From: Sand, Peter
Sent: Friday, December 02, 2011 04:55 PM
To: Andrew, Emily; (b) (6)
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Pilot Evaluation Report

Yeah, (b) (5) the blurb I wrote is with MEC now, I'll let you know what I get back.

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! [redacted].

From: Andrew, Emily
Sent: Friday, December 02, 2011 4:54 PM
To: Sand, Peter; [redacted]
Cc: Falkenstein, Cindy; Lockett, Vania; [redacted]
Subject: Re: DIB Pilot Evaluation Report

I haven't read it yet, but I would say that you should still respond.

From: Sand, Peter
Sent: Friday, December 02, 2011 04:45 PM
To: Andrew, Emily; [redacted]
Cc: Falkenstein, Cindy; Lockett, Vania; [redacted]
Subject: RE: DIB Pilot Evaluation Report

Emily,

[redacted] Or is he doing a separate report?

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: [redacted] pager: [redacted]
[redacted]; 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! [redacted].

From: Andrew, Emily
Sent: Friday, December 02, 2011 4:44 PM
To: [redacted] Sand, Peter; [redacted]
Cc: Falkenstein, Cindy; Lockett, Vania; [redacted]
Subject: Fw: DIB Pilot Evaluation Report

FYI

From: Dean, Nicole M
Sent: Friday, December 02, 2011 04:39 PM
To: [redacted] Goode, Brendan; McDermott, Thomas M; [redacted] Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; [redacted] Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew,

Emily
Subject: DIB Pilot Evaluation Report

<<DIB Pilot Evaluation Report 113011_v1_NO SECTIONS 4 AND 5_DRAFT-FINAL.PDF>>

All,

Here is the DIB pilot final report.

Andrew, Emily

From: Andrew, Emily
Sent: Monday, December 05, 2011 6:46 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Thanks – (b) (5), so I'd rather our CS&C folks chime in.

From: Sand, Peter
Sent: Friday, December 02, 2011 10:03 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Then I'll send MEC this language and note that we are also sending it through NPPD for their clearance.

I didn't mention any specific SOPs - I'm sure he will ask for them as a follow up.

I recall there once was a separate SOP that specifically laid out the development of templates and signatures. I pulled the language I used from SOP 108 and 445.

If he does ask for the actual SOPs, I am going to defer to NPPD because they are NPPD docs.

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: Andrew, Emily
Sent: Friday, December 02, 2011 9:58 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

(b) (5)

(b) (5)

From: Sand, Peter
Sent: Friday, December 02, 2011 9:25 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

Prof. Travis Breaux, from CMU, (b) (5)

(b) (5)

I am also sending to MEC for review.

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: Travis Breaux [redacted]
Sent: Wednesday, November 30, 2011 1:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: [redacted]; pager: [redacted]
[redacted] 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! [redacted].

From: Travis Breaux [redacted]
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,

--

Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Andrew, Emily
To: Falkenstein, Cindy
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines
Date: Monday, December 05, 2011 6:48:25 AM

Cindy – so we are not double working this. Is Kurt also coordinating with Brendan and Tom on the language?

Emily

From: Falkenstein, Cindy
Sent: Friday, December 02, 2011 9:49 AM
To: (b) (6) Sand, Peter; Andrew, Emily
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

All,
Kurt Steiner is the Compliance and Oversight Officer. Kurt is part of our bi-weekly NCPS Privacy Compliance Workgroup. I have received word (b) (5) , and should include some more specific language to address the recent concerns, (b) (5) so hopefully he will be getting back to us on this real soon.

Suggestion might be to run the proposed language by Kurt to see if he can confirm or clarify any of the details.
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: (b) (6)
Sent: Friday, December 02, 2011 9:30 AM
To: Sand, Peter; Andrew, Emily; Falkenstein, Cindy
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

(b) (5)

(b) (6)

DHS Privacy Office
(b) (6)
(b) (6)
Visit our privacy website

From: Sand, Peter
Sent: Friday, December 02, 2011 9:25 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

Prof. Travis Breaux, from CMU, (b) (5)
(b) (5)

I am also sending to MEC for review.

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: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 1:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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! [redacted].

From: Travis Breaux [redacted]
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Andrew, Emily
To: Sand, Peter; (b) (6)
Cc: Falkenstein, Cindy
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines
Date: Monday, December 05, 2011 11:57:55 AM

I just spoke to Cindy – I think we are okay to send it on. (b) (5)

Carole just confirmed that she did send something to leadership on the Tasker. I would say that we should just proceed sine my previous message said if we don't hear from you we will assume you approve. (b) (5)

From: Sand, Peter
Sent: Monday, December 05, 2011 11:45 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

MEC approved the language – here it is again for your review. (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

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: Monday, December 05, 2011 6:46 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Thanks – (b) (5), so I'd rather our CS&C folks chime in.

From: Sand, Peter
Sent: Friday, December 02, 2011 10:03 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Then I'll send MEC this language and note that we are also sending it through NPPD for their clearance.

I didn't mention any specific SOPs – I'm sure he will ask for them as a follow up.

I recall there once was a separate SOP that specifically laid out the development of templates and signatures. I pulled the language I used from SOP 108 and 445.

If he does ask for the actual SOPs, I am going to defer to NPPD because they are NPPD docs.

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: Andrew, Emily
Sent: Friday, December 02, 2011 9:58 AM
To: Sand, Peter; Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

(b) (5)

From: Sand, Peter
Sent: Friday, December 02, 2011 9:25 AM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6)
Subject: [REVIEW] DIB PIlot Evaluation: Question about Privacy guidelines

Emily,

Prof. Travis Breaux, from CMU, (b) (5)

(b) (5)

(b) (5)

I am also sending to MEC for review.

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! [redacted].

From: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 1:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--

Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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: Travis Breaux (b) (6)
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Andrew, Emily
To: Goode, Brendan; McDermott, Thomas M
Cc: (b) (6); Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6); Falkenstein, Cindy
Subject: RE: Draft JCSP PTA
Date: Wednesday, December 07, 2011 10:03:05 AM

Thanks for the input. For now, (b) (5).

Emily

From: Goode, Brendan
Sent: Wednesday, December 07, 2011 9:53 AM
To: McDermott, Thomas M; Andrew, Emily
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) Falkenstein, Cindy
Subject: Re: Draft JCSP PTA

(b) (5)

From: McDermott, Thomas M
Sent: Wednesday, December 07, 2011 09:45 AM
To: Goode, Brendan; Andrew, Emily
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) Falkenstein, Cindy
Subject: RE: Draft JCSP PTA

(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: Goode, Brendan
Sent: Wednesday, December 07, 2011 9:41 AM
To: McDermott, Thomas M; Andrew, Emily
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) Falkenstein, Cindy
Subject: Re: Draft JCSP PTA

(b) (5)

From: McDermott, Thomas M
Sent: Wednesday, December 07, 2011 09:35 AM
To: Goode, Brendan; Andrew, Emily
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) Falkenstein, Cindy
Subject: RE: Draft JCSP PTA

(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: Goode, Brendan
Sent: Wednesday, December 07, 2011 9:17 AM
To: Andrew, Emily
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) McDermott, Thomas M; Falkenstein, Cindy
Subject: Re: Draft JCSP PTA

Thanks Emily.

(b) (5)

(b) (5)

From: Andrew, Emily
Sent: Wednesday, December 07, 2011 09:05 AM
To: Goode, Brendan
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6) McDermott, Thomas M; Falkenstein, Cindy
Subject: RE: Draft JCSP PTA

Brendan,

I made a couple of edits, can you review for accuracy? If you agree, I'll send to PRIV for adjudication.

Thanks
Emily

From: Goode, Brendan
Sent: Monday, December 05, 2011 9:00 PM
To: Andrew, Emily; Falkenstein, Cindy
Cc: (b) (6) Dean, Nicole M; Rock, Lee; Delaney, Laura; (b) (6)
Subject: Draft JCSP PTA

Hi Emily/Cindy-

Attached is a rough draft of the JCSP PTA. Once you have read through it, maybe we can have a short discussion to walk through any questions. (b) (5) (b) (5). I am in a training class tomorrow, but I think we will break between 11:30 – 12:30. Are you free somewhere in between those times?

Some of the key tenants:

(b) (5)

(b) (5)

Thanks,
Brendan

From: Andrew, Emily
To: Sand, Peter
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Joint Cybersecurity Services Pilot (JCSP) - PTA
Date: Wednesday, December 07, 2011 10:44:50 AM

Yes – fast track. I (b) (5) I just sent you the revised.

From: Sand, Peter
Sent: Wednesday, December 07, 2011 10:37 AM
To: Andrew, Emily
Cc: Falkenstein, Cindy; (b) (6)
Subject: Re: Joint Cybersecurity Services Pilot (JCSP) - PTA

Emily - are we (b) (5)

I assume thins is all fast-tracked because the whole pilot is only 180 days?

Pete

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

From: Andrew, Emily
Sent: Wednesday, December 07, 2011 10:17 AM
To: PIA; Richards, Rebecca
Cc: Falkenstein, Cindy; NPPDPrivacy; (b) (6) Sand, Peter
Subject: Joint Cybersecurity Services Pilot (JCSP) - PTA

HQ PRIV,

Please find the attached Joint Cybersecurity Service Pilot PTA for your review and adjudication.

Some of the key tenants:

(b) (5)

(b) (5)

Since this program is set to be implemented on or about January 15, 2012, we ask that you expedite this PTA.

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: Steiner, Kurt
To: Falkenstein, Cindy
Subject: RE: Joint Cybersecurity Services Pilot (JCSP) - PTA
Date: Wednesday, December 07, 2011 1:14:12 PM

(b) (5)

From: Falkenstein, Cindy
Sent: Wednesday, December 07, 2011 12:53 PM
To: Steiner, Kurt
Subject: FW: Joint Cybersecurity Services Pilot (JCSP) - PTA

(b) (5)

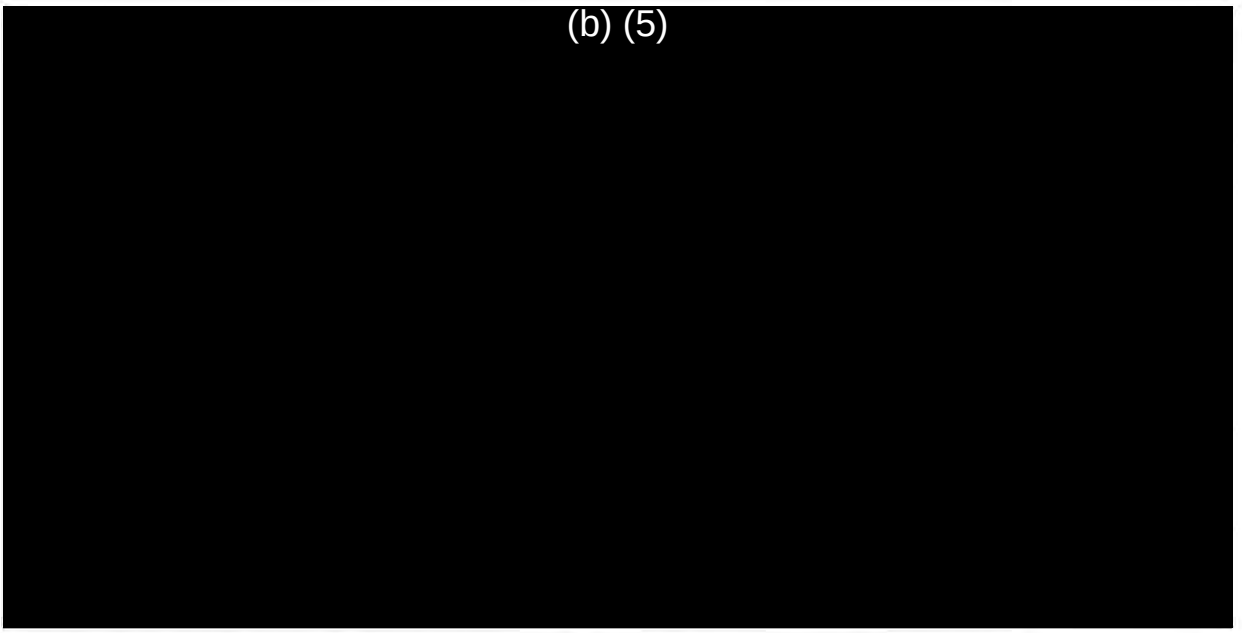
Cindy

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

From: Andrew, Emily
Sent: Wednesday, December 07, 2011 10:18 AM
To: PIA; Richards, Rebecca
Cc: Falkenstein, Cindy; NPPDPrivacy; (b) (6) Sand, Peter
Subject: Joint Cybersecurity Services Pilot (JCSP) - PTA

HQ PRIV,

Please find the attached Joint Cybersecurity Service Pilot PTA for your review and adjudication.



Since this program is set to be implemented on or about January 15, 2012, we ask that you expedite this PTA.

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)

Andrew, Emily

From: Davis, Robert M
Sent: Friday, December 09, 2011 10:35 AM
To: Andrew, Emily
Cc: Falkenstein, Cindy
Subject: RE: DIB
Attachments: DHS TPs re Bloomberg.docx

Here are the talking points Mark used for this story that Bloomberg ran today on its pay site.

By Chris Strohm

Dec. 8 (Bloomberg) -- The Obama administration will extend a test program for sharing classified data on cyberthreats with defense contractors and Internet-service providers, shifting management of the effort to the Homeland Security Department.

The Defense Industrial Base cybersecurity program will be extended for several more months, Mark Weatherford, the Homeland Security Department's new deputy undersecretary for cybersecurity, said in an interview today.

Under the changes to the program, run since being announced in June by the Defense Department, Homeland Security will assume the leading role in interacting with Internet-service providers, said Weatherford, who started in his position last month. The Pentagon will remain the primary contact for defense contractors, he said.

The purpose of the extension is to "get better in the sharing of information" about cybersecurity threats, he said.

Data breaches this year at Sony Corp., Citigroup Inc. and Lockheed Martin Corp. have sharpened government scrutiny of U.S.
network defenses. Several cybersecurity bills circulating in Congress call for wider sharing of information about hacker threats between U.S. agencies and companies.

Under the voluntary program to be overseen by Homeland Security, the government and participating companies exchange sensitive data on cyberattacks and hacker threats to help safeguard networks critical to the military.

The government hasn't disclosed the companies that are involved. Ed McFadden, a spokesman for Verizon Communications Inc., declined to comment, as did Mark Siegel, a spokesman for AT&T Inc.

No Personal Communications

Participating Internet-service providers will provide Homeland Security with information about intrusions and attacks on their networks, and the department will pass data to the Pentagon. Cyberthreat information from the Pentagon -- primarily the National Security Agency -- will be passed through Homeland Security to commercial Internet providers.

The information from Internet providers won't include the content of subscribers' personal communications, the department said. Instead, the data to be shared is limited to summary statistics about the kinds of incidents that are being detected, according to the department.

Putting Homeland Security in charge of dealing with Internet-service providers "is an appropriate way to evolve the program" and intended to reinforce the idea that the department is responsible for working with the owners and operators of non- military critical infrastructure, Weatherford said.

For Related News and Information:
Computer security news: NI ITSECURE <GO> Today's top technology news: TTOP <GO> More technology regulatory news: NI TECHREG <GO> Top government news: GTOP <GO>

--Editors: Michael Shepard, Romaine Bostick

(b) (5)

From: (b) (6)
To: Dean, Nicole M; Goode, Brendan; McDermott, Thomas M; (b) (6) Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily; Royster, Kristin
Subject: RE: JCSP Transition Activities
Date: Monday, December 12, 2011 2:52:05 PM
Attachments: Talking Points -- DIB Pilot 12-8-11.docx

All,

I'm attaching the Talking Points that Kristin developed and Nicole approved, as I don't think everyone has seen them.

Thanks,
(b) (6)

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

From: Dean, Nicole M
Sent: Monday, December 12, 2011 1:53 PM
To: (b) (6) Goode, Brendan; 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily; Royster, Kristin
Subject: RE: JCSP Transition Activities

All,

(b) (5)

Thanks,
Nicole

From: (b) (6)
To: Dean, Nicole M; (b) (6); Goode, Brendan; McDermott, Thomas M; (b) (b) (6); Rock, Lee; Harris, Richard; Menna, Jenny; Kizzee, Carlos; Coose, Matt; Smith, Mike C; Donelan, Sean; Delaney, Laura; (b) (6); Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily; Royster, Kristin
Subject: Re: JCSP Transition Activities
Date: Monday, December 12, 2011 5:42:36 PM

Nicole/Brendan-

Here are my quick notes....

(b) (5)

All-

Please add to or correct any of the above that I may not have captured correctly.

Thanks,

(b) (6)

From: Dean, Nicole M
Sent: Monday, December 12, 2011 01:53 PM
To: (b) (6) Goode, Brendan; 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily; Royster, Kristin
Subject: RE: JCSP Transition Activities

All,
I may or may not make the call tonight. There a few items I would like status on so if I could get notes on these topics I would appreciate it.

(b) (5)

Thanks,
Nicole

From: Andrew, Emily
To: Falkenstein, Cindy
Subject: FW: DOE PIA
Date: Tuesday, December 13, 2011 9:43:34 AM

I will call you first – then (b) (6)

From: Hanley, Jerry (b) (6)
Sent: Tuesday, December 13, 2011 8:26 AM
To: Andrew, Emily
Subject: RE: DOE PIA

Emily, please call at 10:00 if that's good for you.

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

From: Andrew, Emily (b) (6)
Sent: Tuesday, December 13, 2011 6:59 AM
To: Hanley, Jerry
Cc: Sand, Peter
Subject: DOE PIA

Good morning (b) (6),

I wanted to touch base with you (b) (5)
(b) (5)

Do you have any time this morning for a quick call?

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: McDermott, Thomas M
To: Sand, Peter; Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6); Steiner, Kurt
Subject: RE: DIB Eval - CMU prof asking for docs
Date: Wednesday, December 14, 2011 4:33:17 PM

For the DIB Pilot activity, at least to date, (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: Sand, Peter
Sent: Wednesday, December 14, 2011 11:59 AM
To: McDermott, Thomas M; Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6) Steiner, Kurt
Subject: RE: DIB Eval - CMU prof asking for docs

Tom, Kurt, others,

This is what the Professor asked, "Is there documentation of these standard operating procedures that US-CERT uses?"

(b) (5)

I'd like to get back to him soon because he asked Friday of last week.

FYI, this is how I originally responded to him:

Professor,

Rather than developing stand-along privacy guidance, we decided to integrate privacy standards into the same standard operating procedures US-CERT will use to conduct their operations. We felt this would make privacy protection part of an integrated practice.

In one SOP, US-CERT requires analysts to demonstrate minimization of data collection before deploying a new signature, including specific efforts to minimize the potential collection of information that could be considered PII. In a second SOP, US-CERT directs analysts to review all data that is received to determine if it contains information that could be considered PII and if so, to ensure it is pertinent to the analysis and further minimize it as much as possible. Any information could be considered PII that is necessary to understand a cybersecurity issue will be marked and notification sent through the Information Oversight staff to determine if retention of that data is warranted.

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: Monday, December 12, 2011 11:11 AM
To: Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6); Steiner, Kurt
Subject: Re: DIB Eval - CMU prof asking for docs

Adding Kurt Steiner from US-CERT.

(b) (5)

Going forward, the information would be handled under the new procedures being updated.

Thomas McDermott
Office of the General Counsel

U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
Sent: Friday, December 09, 2011 08:38 AM
To: Goode, Brendan; McDermott, Thomas M
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)
Subject: FW: DIB Eval - CMU prof asking for docs

Brendan / Tom,

Pete Sand has been working with the CMU professor on the DIB evaluation. The professor asked questions about SOPs (b) (5)

(b) (5)

Emily

From: Sand, Peter
Sent: Friday, December 09, 2011 6:45 AM
To: Andrew, Emily; Falkenstein, Cindy
Subject: DIB Eval - CMU prof asking for docs

Emily,

Looks like his privacy eval is still going on. He's asking about the actual SOPs.

(b) (5)

Could you run this by your people and let me know how I should respond?

(b) (5)

Pete

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

From: Travis Breaux [redacted]
Sent: Friday, December 09, 2011 03:11 AM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Peter,

This definitely helps. Thank you. Is there documentation of these standard operating procedures that US-CERT uses?

Again, thank you for your help.

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Dec 8, 2011, at 11:35 AM, Sand, Peter wrote:

Professor,

Did that answer your question? Anything else I can help with?

Pete

Peter E. Sand, J.D., CIPP/G/IT
Director of Privacy Technology
Department of Homeland Security
voice: [redacted] pager: [redacted]
[redacted] 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! [redacted].

From: Sand, Peter
Sent: Tuesday, December 06, 2011 7:39 AM
To: [redacted]
Subject: Re: Privacy guidelines

Professor,

Rather than developing stand-along privacy guidance, we decided to integrate privacy standards into the same standard operating procedures US-CERT will use to conduct their operations. We felt this would make privacy protection part of an integrated practice.

In one SOP, US-CERT requires analysts to demonstrate minimization of data collection before deploying a new signature, including specific efforts to minimize the potential collection of information that could be considered PII. In a second SOP, US-CERT directs analysts to review all data that is received to determine if it contains information that could be considered PII and if so, to ensure it is pertinent to the analysis and further minimize it as much as possible. Any information could be considered PII that is necessary to understand a cybersecurity issue will be marked and notification sent through the Information Oversight staff to determine if retention of that data is warranted.

Again, apologies for the delay,

Pete

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

From: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 01:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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: Travis Breaux (b) (6)
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Andrew, Emily
To: Falkenstein, Cindy
Subject: FW: DIB Eval - CMU prof asking for docs
Date: Wednesday, December 14, 2011 7:47:10 PM

I'm learning something new every day. (b) (5) Guess not.

From: McDermott, Thomas M
Sent: Wednesday, December 14, 2011 4:33 PM
To: Sand, Peter; Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6) Steiner, Kurt
Subject: RE: DIB Eval - CMU prof asking for docs

For the DIB Pilot activity, at least to date, (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: Sand, Peter
Sent: Wednesday, December 14, 2011 11:59 AM
To: McDermott, Thomas M; Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6) Steiner, Kurt
Subject: RE: DIB Eval - CMU prof asking for docs

Tom, Kurt, others,

This is what the Professor asked, "Is there documentation of these standard operating procedures that US-CERT uses?"

(b) (5)

I'd like to get back to him soon because he asked Friday of last week.

FYI, this is how I originally responded to him:

Professor,

Rather than developing stand-along privacy guidance, we decided to integrate privacy standards into the same standard operating procedures US-CERT will use to conduct their operations. We felt this would make privacy protection part of an integrated practice.

In one SOP, US-CERT requires analysts to demonstrate minimization of data collection before deploying a new signature, including specific efforts to minimize the potential collection of information that could be considered PII. In a second SOP, US-CERT directs analysts to review all data that is received to determine if it contains information that could be considered PII and if so, to ensure it is pertinent to the analysis and further minimize it as much as possible. Any information could be considered PII that is necessary to understand a cybersecurity issue will be marked and notification sent through the Information Oversight staff to determine if retention of that data is warranted.

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: Monday, December 12, 2011 11:11 AM
To: Andrew, Emily; Goode, Brendan
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6) Steiner, Kurt
Subject: Re: DIB Eval - CMU prof asking for docs

Adding Kurt Steiner from US-CERT.

(b) (5)

(b) (5)

Going forward, the information would be handled under the new procedures being updated.

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
Sent: Friday, December 09, 2011 08:38 AM
To: Goode, Brendan; McDermott, Thomas M
Cc: Falkenstein, Cindy; Sand, Peter; (b) (6)
Subject: FW: DIB Eval - CMU prof asking for docs

Brendan / Tom,

Pete Sand has been working with the CMU professor on the DIB evaluation. The professor asked questions about SOPs (b) (5)
(b) (5)

Emily

From: Sand, Peter
Sent: Friday, December 09, 2011 6:45 AM
To: Andrew, Emily; Falkenstein, Cindy
Subject: DIB Eval - CMU prof asking for docs

Emily,

Looks like his privacy eval is still going on. He's asking about the actual SOPs.

(b) (5)

Could you run this by your people and let me know how I should respond?

(b) (5)

Pete

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

From: Travis Breaux (b) (6)
Sent: Friday, December 09, 2011 03:11 AM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Peter,

This definitely helps. Thank you. Is there documentation of these standard operating procedures that US-CERT uses?

Again, thank you for your help.
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Dec 8, 2011, at 11:35 AM, Sand, Peter wrote:

Professor,

Did that answer your question? Anything else I can help with?

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
Sent: Tuesday, December 06, 2011 7:39 AM
To: (b) (6)

Subject: Re: Privacy guidelines

Professor,

Rather than developing stand-along privacy guidance, we decided to integrate privacy standards into the same standard operating procedures US-CERT will use to conduct their operations. We felt this would make privacy protection part of an integrated practice.

In one SOP, US-CERT requires analysts to demonstrate minimization of data collection before deploying a new signature, including specific efforts to minimize the potential collection of information that could be considered PII. In a second SOP, US-CERT directs analysts to review all data that is received to determine if it contains information that could be considered PII and if so, to ensure it is pertinent to the analysis and further minimize it as much as possible. Any information could be considered PII that is necessary to understand a cybersecurity issue will be marked and notification sent through the Information Oversight staff to determine if retention of that data is warranted.

Again, apologies for the delay,

Pete

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

From: Travis Breaux (b) (6)
Sent: Wednesday, November 30, 2011 01:47 PM
To: Sand, Peter
Subject: Re: Privacy guidelines

Hi Pete,

I hope you had a great Thanksgiving holiday. I want to ping you again on this question, below. Thanks again for your help!

> I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Best,
--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

On Nov 15, 2011, at 7:24 AM, Sand, Peter wrote:

Travis,

Sorry for the delay - I did get your email and will follow up shortly....

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: Travis Breaux (b) (6)
Sent: Wednesday, November 09, 2011 2:32 PM
To: Sand, Peter
Subject: Privacy guidelines

Hi Pete,

Thanks for taking the time the other day to walk me through the DHS PIA process.

I saw in the E2 PIA that US-CERT uses privacy guidelines for reviewing prospective attack signatures before they go "live". Would it be possible to review those guidelines for their applicability to the DIB program?

Thanks,

--
Travis Breaux, Ph.D.
Carnegie Mellon University
http://www.cs.cmu.edu/~breaux

From: Harris, Richard
To: McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; Goode, Brendan; (b) (6)
Subject: RE: Cybersecurity and NSS
Date: Thursday, December 15, 2011 4:43:31 PM

We can cover those topics. Has the meeting time/location/call-in been set?

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 3:05 PM
To: Rock, Lee
Cc: Andrew, Emily; Falkenstein, Cindy; Harris, Richard; Jacobs, Michael; Steiner, Kurt; Goode, Brendan
Subject: RE: Cybersecurity and NSS

(b) (5)

From: Rock, Lee
Sent: Thursday, December 15, 2011 2:12 PM
To: McDermott, Thomas M; Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Harris, Richard; Steiner, Kurt
Subject: RE: Cybersecurity and NSS

Let us know what support you need and we will try to accommodate.

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 1:46 PM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Rock, Lee; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

I think we need (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: Andrew, Emily
Sent: Thursday, December 15, 2011 1:21 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

Did you all want to still try and get together later this afternoon to discuss the getbacks? MEC and I are both out next week so it would be great if we could get this finalized by tomorrow.

Emily

From: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 5:16 PM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Ok, tahnks gusy.

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: McDermott, Thomas M
Sent: Wednesday, December 14, 2011 5:15 PM
To: Callahan, Mary Ellen; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

(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: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 4:21 PM
To: Andrew, Emily; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

I think this is a really good first cut! And close to final cut! The only addition (b) (5)

Thanks all! nice work.

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: Wednesday, December 14, 2011 3:45 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Here's my first attempt at a response. I'm not 100% (b) (5)

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: Callahan, Mary Ellen
Sent: Tuesday, December 13, 2011 9:00 AM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

Let's shoot for 11am tomorrow? (b) (6) is getting a #. Tx.

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

From: McDermott, Thomas M
Sent: Tuesday, December 13, 2011 08:33 AM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6)
<(b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

(b) (6)

I can hopefully participate in a call tomorrow between 11 and 4.

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
Sent: Tuesday, December 13, 2011 06:20 AM
To: Callahan, Mary Ellen; McDermott, Thomas M <(b) (6) Goode, Brendan
Subject: RE: Cybersecurity and NSS

(b) (5)

I can set up a call if you could all let me know of your availability.

Emily

From: Callahan, Mary Ellen
Sent: Monday, December 12, 2011 8:03 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; Callahan, Mary Ellen
Subject: Cybersecurity and NSS

I just got a call from (b) (6) asking about our "responses" to that meeting the other day. She said she would like something written, at least identifying issues on the way, being worked on, etc. I don't know that we ever talked about how to respond – should we talk or try to figure out a plan? Btw, I have (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: Falkenstein, Cindy
To: (b) (6)
Subject: Classification for JCSP
Date: Friday, December 16, 2011 3:03:00 PM

Hi (b) (6)
I'm drafting a PIA (b) (5)

Are you here at Glebe today and would you have ~5 minutes to explain this to me?
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) |
(b) (6) | DHS Privacy Website | NPPD Privacy Intranet

Andrew, Emily

From: Andrew, Emily
Sent: Friday, December 16, 2011 2:37 PM
To: Goode, Brendan; Harris, Richard; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Jacobs, Michael; Steiner, Kurt; (b) (6) Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS
Attachments: Privacy Oversight.DHS task_20111214.docx; Privacy Oversight.taskdiv.docx

Here's the attachment. We just need (b) (5)

Please feel free to give me a call if you have any questions.

Emily
(b) (6)

From: Goode, Brendan
Sent: Friday, December 16, 2011 2:27 PM
To: Harris, Richard; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; (b) (6) Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS

Emily's e-mail was requesting a (b) (5) Please reference earlier attachment.

From: Harris, Richard
Sent: Friday, December 16, 2011 2:22 PM
To: Goode, Brendan; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; (b) (6) Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS

Brendan – not sure what you are looking for.... (b) (5)

From: Goode, Brendan
Sent: Friday, December 16, 2011 1:10 PM
To: Falkenstein, Cindy; Harris, Richard; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; (b) (6) Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS
Importance: High

Lee/Rick-

Do we have a timeline for when we can get a response back to Cindy and Emily? (b) (5).

Thanks,
Brendan

From: Falkenstein, Cindy
Sent: Thursday, December 15, 2011 5:21 PM
To: Harris, Richard; McDermott, Thomas M; Rock, Lee

Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; Goode, Brendan; (b) (6) Callahan, Mary Ellen
Subject: RE: Cybersecurity and NSS

Rick/Lee,
I don't believe you all received the documents that relate to this thread. I'm attaching Emily's first cut at responding and this is where we could use (b) (5)

Attached is the (b) (5) is Privacy's response.
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

From: Harris, Richard
Sent: Thursday, December 15, 2011 4:43 PM
To: McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; Goode, Brendan; (b) (6)
Subject: RE: Cybersecurity and NSS

We can cover those topics. Has the meeting time/location/call-in been set?

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 3:05 PM
To: Rock, Lee
Cc: Andrew, Emily; Falkenstein, Cindy; Harris, Richard; Jacobs, Michael; Steiner, Kurt; Goode, Brendan
Subject: RE: Cybersecurity and NSS

(b) (5)

From: Rock, Lee
Sent: Thursday, December 15, 2011 2:12 PM
To: McDermott, Thomas M; Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Harris, Richard; Steiner, Kurt
Subject: RE: Cybersecurity and NSS

Let us know what support you need and we will try to accommodate.

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 1:46 PM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Rock, Lee; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

I think we need (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: Andrew, Emily
Sent: Thursday, December 15, 2011 1:21 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

Did you all want to still try and get together later this afternoon to discuss the getbacks? MEC and I are both out next week so it would be great if we could get this finalized by tomorrow.

Emily

From: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 5:16 PM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Ok, tahnks gusy.

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: McDermott, Thomas M
Sent: Wednesday, December 14, 2011 5:15 PM
To: Callahan, Mary Ellen; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

(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: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 4:21 PM
To: Andrew, Emily; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

I think this is a really good first cut! And close to final cut! The only addition (b) (5)

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: Wednesday, December 14, 2011 3:45 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Here's my first attempt at a response. I'm not 100% (b) (5)

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: Callahan, Mary Ellen
Sent: Tuesday, December 13, 2011 9:00 AM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

Let's shoot for 11am tomorrow? (b) (6) is getting a #. Tx.

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

From: McDermott, Thomas M
Sent: Tuesday, December 13, 2011 08:33 AM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6) < (b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

(b) (6)

I can hopefully participate in a call tomorrow between 11 and 4.

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
Sent: Tuesday, December 13, 2011 06:20 AM
To: Callahan, Mary Ellen; McDermott, Thomas M < (b) (6) ; Goode, Brendan
Subject: RE: Cybersecurity and NSS

(b) (5)

I can set up a call if you could all let me know of your availability.

Emily

From: Callahan, Mary Ellen
Sent: Monday, December 12, 2011 8:03 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; Callahan, Mary Ellen
Subject: Cybersecurity and NSS

00231

I just got a call from (b) (6) asking about our "responses" to that meeting the other day. She said she would like something written, at least identifying issues on the way, being worked on, etc. I don't know that we ever talked about how to respond – should we talk or try to figure out a plan? Btw, (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: Andrew, Emily
To: Falkenstein, Cindy; Lockett, Vania
Subject: FW: Cybersecurity and NSS
Date: Friday, December 16, 2011 4:06:22 PM

FYI – I'm hoping US-CERT gets something today!

From: Callahan, Mary Ellen
Sent: Friday, December 16, 2011 3:55 PM
To: Andrew, Emily
Subject: RE: Cybersecurity and NSS

No, I hadn't promised that, just told him the approach. [redacted (b) (5)] if they can send directly, that would be great! 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: [redacted (b) (6)]
Fax: [redacted (b) (6)]
E-mail: [redacted (b) (6)]
Website: www.dhs.gov/privacy

From: Andrew, Emily
Sent: Friday, December 16, 2011 3:41 PM
To: Callahan, Mary Ellen
Subject: RE: Cybersecurity and NSS

Okay – so we should send to him to review before sending to [redacted (b) (6)]

From: Callahan, Mary Ellen
Sent: Friday, December 16, 2011 3:31 PM
To: Andrew, Emily
Subject: Re: Cybersecurity and NSS

I talked to [redacted (b)(3)-P.L. 86-36] the day we talked, told him our approach. He was appreciative, and said he wd do the same. You guys go ahead.

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

From: Andrew, Emily

Sent: Friday, December 16, 2011 02:47 PM
To: Callahan, Mary Ellen
Subject: FW: Cybersecurity and NSS

Mec- as you can see we are still working this and I hope to get something back to you today. Once we get the list finalized, [redacted] (b) (5) [redacted] I believe that you were going to [redacted] (b) (5) [redacted]

If you are out of pocket after we get this finalized one of us can send to [redacted] (b) (6) [redacted] I'm out on leave next week too and will have very limited access to BB Tues – Thurs but we will make sure it gets done.

From: Andrew, Emily
Sent: Friday, December 16, 2011 2:37 PM
To: Goode, Brendan; Harris, Richard; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Jacobs, Michael; Steiner, Kurt; [redacted] (b) (6) [redacted] Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS

Here's the attachment. We just need to [redacted] (b) (5) [redacted]

Please feel free to give me a call if you have any questions.

Emily
[redacted] (b) (6) [redacted]

From: Goode, Brendan
Sent: Friday, December 16, 2011 2:27 PM
To: Harris, Richard; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; [redacted] (b) (6) [redacted] Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS

Emily's e-mail was requesting a [redacted] (b) (5) [redacted]
Please reference earlier attachment.

From: Harris, Richard
Sent: Friday, December 16, 2011 2:22 PM
To: Goode, Brendan; Falkenstein, Cindy; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; [redacted] (b) (6) [redacted] Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS

Brendan – not sure what you are looking for.... [redacted] (b) (5) [redacted]

From: Goode, Brendan
Sent: Friday, December 16, 2011 1:10 PM

To: Falkenstein, Cindy; Harris, Richard; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; (b) (6) Callahan, Mary Ellen; Austin, Mark
Subject: RE: Cybersecurity and NSS
Importance: High

Lee/Rick-

Do we have a timeline for when we can get a response back to Cindy and Emily? (b) (5)

Thanks,
Brendan

From: Falkenstein, Cindy
Sent: Thursday, December 15, 2011 5:21 PM
To: Harris, Richard; McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Jacobs, Michael; Steiner, Kurt; Goode, Brendan; (b) (6) Callahan, Mary Ellen
Subject: RE: Cybersecurity and NSS

Rick/Lee,
I don't believe you all received the documents that relate to this thread. I'm attaching Emily's first cut at responding and this is where we could use (b) (5)

Attached is the (b) (5) is Privacy's response.
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

From: Harris, Richard
Sent: Thursday, December 15, 2011 4:43 PM
To: McDermott, Thomas M; Rock, Lee
Cc: Andrew, Emily; Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; Goode, Brendan; (b) (6)
Subject: RE: Cybersecurity and NSS

We can cover those topics. Has the meeting time/location/call-in been set?

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 3:05 PM
To: Rock, Lee

Cc: Andrew, Emily; Falkenstein, Cindy; Harris, Richard; Jacobs, Michael; Steiner, Kurt; Goode, Brendan
Subject: RE: Cybersecurity and NSS

(b) (5)

From: Rock, Lee
Sent: Thursday, December 15, 2011 2:12 PM
To: McDermott, Thomas M; Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Harris, Richard; Steiner, Kurt
Subject: RE: Cybersecurity and NSS

Let us know what support you need and we will try to accommodate.

From: McDermott, Thomas M
Sent: Thursday, December 15, 2011 1:46 PM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6) Goode, Brendan; Rock, Lee; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

I think we need (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: Andrew, Emily
Sent: Thursday, December 15, 2011 1:21 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan
Cc: Falkenstein, Cindy; (b) (6)
Subject: RE: Cybersecurity and NSS

Did you all want to still try and get together later this afternoon to discuss the getbacks? MEC and I are both out next week so it would be great if we could get this finalized by tomorrow.

Emily

From: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 5:16 PM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Ok, tahnks gusy.

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: McDermott, Thomas M
Sent: Wednesday, December 14, 2011 5:15 PM
To: Callahan, Mary Ellen; Andrew, Emily; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

(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: Callahan, Mary Ellen
Sent: Wednesday, December 14, 2011 4:21 PM
To: Andrew, Emily; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

I think this is a really good first cut! And close to final cut! The only addition (b) (5)

Thanks all! nice work.

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: Wednesday, December 14, 2011 3:45 PM
To: Callahan, Mary Ellen; McDermott, Thomas M; (b) (6) Goode, Brendan; Falkenstein, Cindy
Subject: RE: Cybersecurity and NSS

Here's my first attempt at a response. I'm not 100% (b) (5)

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: Callahan, Mary Ellen
Sent: Tuesday, December 13, 2011 9:00 AM
To: McDermott, Thomas M; Andrew, Emily; (b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

Let's shoot for 11am tomorrow? (b) (6) is getting a #. Tx.

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

From: McDermott, Thomas M
Sent: Tuesday, December 13, 2011 08:33 AM
To: Andrew, Emily; Callahan, Mary Ellen; (b) (6) <(b) (6) Goode, Brendan
Subject: Re: Cybersecurity and NSS

(b) (6)

I can hopefully participate in a call tomorrow between 11 and 4.

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
Sent: Tuesday, December 13, 2011 06:20 AM
To: Callahan, Mary Ellen; McDermott, Thomas M <(b) (6) Goode, Brendan
Subject: RE: Cybersecurity and NSS

Can we assume (b) (5)

I can set up a call if you could all let me know of your availability.

Emily

From: Callahan, Mary Ellen
Sent: Monday, December 12, 2011 8:03 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; Callahan, Mary Ellen
Subject: Cybersecurity and NSS

I just got a call from (b) (6) asking about our "responses" to that meeting the other day. She said she would like something written, at least identifying issues on the way, being worked on, etc. I

don't know that we ever talked about how to respond – should we talk or try to figure out a plan? Btw, I have [redacted] (b) (5) [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: [redacted] (b) (6) [redacted]
Fax: [redacted] (b) (6) [redacted]
E-mail: [redacted] (b) (6) [redacted]
Website: www.dhs.gov/privacy

Andrew, Emily

From: Falkenstein, Cindy
Sent: Friday, December 16, 2011 4:06 PM
To: (b) (6)
Cc: Andrew, Emily; Lockett, Vania
Subject: RE: Classification for JCSP

Jennifer,
Can you also add Emily Andrew and Vania Lockett to the guidance email on the C-LAN?
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

From: (b) (6)
Sent: Friday, December 16, 2011 3:52 PM
To: Falkenstein, Cindy
Cc: (b) (6)
Subject: RE: Classification for JCSP

Hi Cindy,

I can send you the current guidance on the CLAN. What is your email address?

/R
(b) (6)

From: Falkenstein, Cindy
Sent: Friday, December 16, 2011 3:05 PM
To: (b) (6)
Subject: FW: Classification for JCSP

Hi (b) (6),
I just got (b) (6) out of office email and was wondering if you might be able to help me with the request below?
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) |
DHS Privacy Website | NPPD Privacy Intranet

From: Falkenstein, Cindy
Sent: Friday, December 16, 2011 3:04 PM

00241

To: (b) (6)
Subject: Classification for JCSP

Hi (b) (6)
I'm drafting a PIA (b) (5)
(b) (5)

Are you here at Glebe today and would you have ~5 minutes to explain this to me?
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

From: Andrew, Emily
To: Lockett, Vania
Cc: Falkenstein, Cindy
Subject: FW: NSS Privacy Questions
Date: Monday, December 19, 2011 6:52:21 AM

Vania - FYI - this is a hot topic for today. We [redacted (b) (5)] If they do not get it they will report that we have failed to turn it in.

This should really come from MEC but she's on leave. If I'm not available to send to [redacted (b) (6)] (not sure where I'll be when it finally gets done), I'll request that Tom send it over.

Emily

-----Original Message-----
From: Andrew, Emily
Sent: Monday, December 19, 2011 6:49 AM
To: McDermott, Thomas M; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Rock, Lee; Harris, Richard
Cc: [redacted (b) (6)]
Subject: RE: NSS Privacy Questions

If [redacted (b) (5)], your response is accurate.

-----Original Message-----
From: McDermott, Thomas M
Sent: Sunday, December 18, 2011 2:19 PM
To: Andrew, Emily; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Rock, Lee; Harris, Richard
Cc: [redacted (b) (6)]
Subject: NSS Privacy Questions
Importance: High

[redacted (b) (5)]

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: [redacted (b) (6)]
bb: [redacted (b) (6)]
Sent from my blackberry device

Andrew, Emily

From: Rock, Lee
Sent: Monday, December 19, 2011 7:14 AM
To: Andrew, Emily; McDermott, Thomas M; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Harris, Richard
Cc: (b) (6)
Subject: RE: NSS Privacy Questions

We will get you a reviewed version this morning.

-----Original Message-----
From: Andrew, Emily
Sent: Monday, December 19, 2011 6:49 AM
To: McDermott, Thomas M; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Rock, Lee; Harris, Richard
Cc: (b) (6)
Subject: RE: NSS Privacy Questions

If (b) (5), your response is accurate.

-----Original Message-----
From: McDermott, Thomas M
Sent: Sunday, December 18, 2011 2:19 PM
To: Andrew, Emily; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Rock, Lee; Harris, Richard
Cc: (b) (6)
Subject: NSS Privacy Questions
Importance: High

(b) (5)

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Falkenstein, Cindy
To: Andrew, Emily
Cc: Lockett, Vania
Subject: Re: DIB Draft Recommendations - updated version to NSS
Date: Monday, December 19, 2011 1:54:41 PM

(b) (5). Lee is in a meeting with Nicole and the AS. He will get someone to finish it up for him.

(b) (5)

Cindy V. Falkenstein
Senior Privacy Analyst
U.S. Dept. Of Homeland Security
(b) (6)
Tel; 7 (b) (6)
Cell: (b) (6)

From: Falkenstein, Cindy
Sent: Monday, December 19, 2011 01:37 PM
To: Andrew, Emily
Subject: RE: DIB Draft Recommendations - updated version to NSS

Vania and I just spoke. We have not heard to see if Tom has received anything, so I will go see if Lee is still around (saw him earlier when I was talking to Mike Jacobs and (b) (6)

I'll let you know what I find – give me 10 min's.

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: Monday, December 19, 2011 1:32 PM
To: Falkenstein, Cindy
Cc: Lockett, Vania
Subject: Re: DIB Draft Recommendations - updated version to NSS

If we can only get US-CERT to look at it. This includes Kurt.

From: Falkenstein, Cindy
Sent: Monday, December 19, 2011 01:02 PM
To: Andrew, Emily
Cc: Lockett, Vania
Subject: RE: DIB Draft Recommendations - updated version to NSS

Yes,
I was just in the SCIF so will look for it.
Vania, let's coordinate so we don't send it to Tom twice.
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

From: Andrew, Emily
Sent: Monday, December 19, 2011 12:06 PM
To: Lockett, Vania; Falkenstein, Cindy
Subject: Fw: DIB Draft Recommendations - updated version to NSS

I'm going to be out of pocket for a few hours. If this get finalized can you both make sure it gets sent out. Tom would be the appropriate person to send.

From: McDermott, Thomas M
Sent: Monday, December 19, 2011 11:40 AM
To: Andrew, Emily; Harris, Richard; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS

(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: Monday, December 19, 2011 7:13 AM
To: Harris, Richard; McDermott, Thomas M; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS

I've updated the version to add comments in the areas we need assistance. Can we get comments

From: Falkenstein, Cindy
To: McDermott, Thomas M
Cc: Lockett, Vania
Subject: RE: NSS Privacy Questions
Date: Monday, December 19, 2011 1:13:53 PM

Tom,
(b) (5)
Let us know if you need for me to do anything.
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
N 1110 N. Glebe Rd. (b) (6) | Arlington VA 22201 | (b) (6) (O) | (b) (6) (BB) |
2 (b) (6) | DHS Privacy Website | NPPD Privacy Intranet

-----Original Message-----
From: McDermott, Thomas M
Sent: Sunday, December 18, 2011 2:19 PM
To: Andrew, Emily; Falkenstein, Cindy; Dean, Nicole M; Goode, Brendan; Rock, Lee; Harris, Richard
Cc: (b) (6)
Subject: NSS Privacy Questions
Importance: High

(b) (5)

Thomas McDermott
Office of the General Counsel
U.S. Department of Homeland Security
ph: (b) (6)
bb: (b) (6)
Sent from my blackberry device

From: Andrew, Emily
To: Lockett, Vania
Subject: FW: DIB Draft Recommendations - updated version to NSS
Date: Monday, December 19, 2011 3:48:16 PM
Attachments: Privacy Oversight DHS task 20111219) (tmm 12-19-11 comments) EA20111219.docx

Let's see (b) (5) We still need Kurt to respond. Feel free to reach out to him.

From: McDermott, Thomas M
Sent: Monday, December 19, 2011 3:00 PM
To: Rock, Lee; Andrew, Emily; Harris, Richard; Goode, Brendan; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Lockett, Vania
Subject: RE: DIB Draft Recommendations - updated version to NSS

(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: Rock, Lee
Sent: Monday, December 19, 2011 2:53 PM
To: Andrew, Emily; McDermott, Thomas M; Harris, Richard; Goode, Brendan; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Lockett, Vania
Subject: RE: DIB Draft Recommendations - updated version to NSS

(b) (5)

From: Andrew, Emily
Sent: Monday, December 19, 2011 2:29 PM
To: McDermott, Thomas M; Harris, Richard; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; (b) (6) Lockett, Vania
Subject: FW: DIB Draft Recommendations - updated version to NSS
Importance: High

Tom – I've responded to your (b) (5). Did Jenn give you a specific deadline for today? I know she told MEC that if she didn't get them, she would just report us as non-responsive for this

task at the IPC tomorrow.

US-CERT – can you give us some idea when we should expect comments?

Thanks
Emily

From: McDermott, Thomas M
Sent: Monday, December 19, 2011 11:40 AM
To: Andrew, Emily; Harris, Richard; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS

(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: Monday, December 19, 2011 7:13 AM
To: Harris, Richard; McDermott, Thomas M; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS

I've updated the version to add comments in the areas we need assistance. Can we get comments back this morning?

Thanks
Emily

From: Harris, Richard
Sent: Friday, December 16, 2011 3:52 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; Rock, Lee
Cc: Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; (b) (6) Austin, Mark
Subject: RE: DIB Draft Recommendations

We will do our best to provide input asap. Our building will be experiencing a power outage in 9

Andrew, Emily

From: McDermott, Thomas M
Sent: Monday, December 19, 2011 11:40 AM
To: Andrew, Emily; Harris, Richard; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS
Attachments: Privacy Oversight DHS task_20111219) (tmm 12-19-11 comments).docx

(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: Monday, December 19, 2011 7:13 AM
To: Harris, Richard; McDermott, Thomas M; Goode, Brendan; Rock, Lee; Steiner, Kurt; (b) (6) Austin, Mark; Jacobs, Michael
Cc: Falkenstein, Cindy; Lockett, Vania; (b) (6)
Subject: RE: DIB Draft Recommendations - updated version to NSS

I've updated the version to add comments in the areas we need assistance. Can we get comments back this morning?

Thanks
Emily

From: Harris, Richard
Sent: Friday, December 16, 2011 3:52 PM
To: Andrew, Emily; McDermott, Thomas M; Goode, Brendan; Rock, Lee
Cc: Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; (b) (6) Austin, Mark
Subject: RE: DIB Draft Recommendations

We will do our best to provide input asap. Our building will be experiencing a power outage in 9 minutes, but we will do the best we can.

From: Andrew, Emily
Sent: Friday, December 16, 2011 3:48 PM
To: McDermott, Thomas M; Goode, Brendan; Rock, Lee
Cc: Falkenstein, Cindy; Jacobs, Michael; Steiner, Kurt; (b) (6) Austin, Mark; Harris, Richard
Subject: FW: DIB Draft Recommendations

Mary Ellen talked to (b)(3)-P.L. 86-36, he was appreciative of our offer to collaborate and he said he would do the same. We need ours finalized today so we can socialize with (b) (6) (DOD) and (b)(3)-P.L. 86 (NSA) and get it back by Monday.

Andrew, Emily

From: Falkenstein, Cindy
Sent: Saturday, December 17, 2011 2:07 PM
To: Andrew, Emily
Subject: RE: Appendix
Attachments: DRAFT PIA NCSD Information Sharing 20111216.docx

I have the overview mostly finished – [redacted] remember we struggled with that before. I will put it in and we can hash it out with Brendan/ [redacted] and Becky.

I had worked on some of the body, but not cleaned it up…I will keep working if I have any more downtime this weekend. ☺

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] | Arlington VA 22201 | [redacted] (O) | [redacted] (BB) |
[redacted] | DHS Privacy Website | NPPD Privacy Intranet

From: Andrew, Emily
Sent: Saturday, December 17, 2011 6:27 AM
To: Falkenstein, Cindy
Subject: Re: Appendix

Work in progress. Can you send me what you have so far? I won't get to it today may have some time tomorrow.

From: Falkenstein, Cindy
Sent: Friday, December 16, 2011 06:23 PM
To: Andrew, Emily
Subject: Re: Appendix

This is great!
Thanks,
Cindy

Cindy V. Falkenstein
Senior Privacy Analyst
U.S. Dept. Of Homeland Security
[redacted]
Tel; [redacted]
Cell: [redacted]

From: Andrew, Emily
Sent: Friday, December 16, 2011 04:38 PM
To: Richards, Rebecca; Falkenstein, Cindy
Cc: Lockett, Vania
Subject: Appendix

Becky – this is still work in progress. Let me know what you [redacted]

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 (b) (6) **Date** Friday, January 13, 2012 11:31:43 AM
To Goode, Brendan; McDermott, Thomas M
Cc
Subject MOA

Good Morning,

(b) (6) has reviewed the MOA, but we still require Legal review before the document is signed. AT&T has two attorneys that are cleared to review the MOA and both are out of the office today. I will work hard to get the MOA signed early next week. Will this delay impact the January 15th transition?

(b) (6)

(b) (6)

AT&T Corp., Government Solutions
*Rethink Possible*SM

Information Assurance Programs (IAP)
(b) (6) (after hours only)

att.com

Please consider the environment before printing this e-mail.

"This email and any files transmitted with it are AT&T property, are confidential, and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing, or copying of this email is strictly prohibited."

From: McConnell, Bruce
Sent: Monday, March 19, 2012 8:59 AM
To: McDermott, Thomas M; Stempfley, Roberta; Goode, Brendan
Cc: Parkinson, Deborah
Subject: RE: DIB Proposal Legal Authorities Memos

(b) (5)

From: McDermott, Thomas M
Sent: Friday, March 16, 2012 5:07 PM
To: McConnell, Bruce; Stempfley, Roberta; Goode, Brendan
Cc: Parkinson, Deborah
Subject: RE: DIB Proposal Legal Authorities Memos

(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: McConnell, Bruce
Sent: Friday, March 16, 2012 12:19 PM
To: McDermott, Thomas M; Stempfley, Roberta; Goode, Brendan
Cc: Parkinson, Deborah
Subject: RE: DIB Proposal Legal Authorities Memos

I think we should ask for an extension until COB Monday.

From: McDermott, Thomas M
Sent: Friday, March 16, 2012 12:12 PM
To: Stempfley, Roberta; McConnell, Bruce; Goode, Brendan
Cc: Parkinson, Deborah
Subject: FW: DIB Proposal Legal Authorities Memos

(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, March 05, 2012 7:59 PM
To: McDermott, Thomas M; Stempfley, Roberta (b) (6)
Subject: RE: DIB Proposal Legal Authorities Memos

Tom,

(b) (5)

Thanks,
(b) (6)

From: (b) (6)
Sent: Monday, March 05, 2012 7:44 PM
To: 'Rosenbach, Eric'; (b) (6) 'Stempfley, Bobbie'; 'McDermott, Thomas M (b) (6)
'Goode, Brendan'; (b)(3)-P.L. 86-36 (b) (6) (b)(3)-P.L. 86-36 (b) (6)
Subject: DIB Proposal Legal Authorities Memos

All,

(b) (5)

Feel free to contact me if you have any questions or concerns.

Thanks,
(b) (6)

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

00255
(b) (6) (direct)
(b) (6) 6 (secure)

From (b) (6), **Date** Wednesday, August 10, 2011 2:30:11 PM
To thomas.m.mcdermot (b) (6)
Cc (b) (6),
Subject Follow Up from Last Week's DIB Pilot Meeting

Tom,
It was good seeing you last week at the DIB Pilot discussion. I know you had the opportunity to hear our interim results summary and feedback on the DIB pilot. I just wanted to follow up and offer to provide you with any other information you need regarding (b) (4), (b) (7) perspective on the Defense Industrial Base pilot and the benefits we believe it brings to our suppliers. At your convenience I would be happy to meet with you or others from your organization to talk about our DIB experiences, our approach to the "advance persistent threat" and how we are protecting our own (b) (4), (b) (7).

If we can be of assistance to you, please let me know.

Very respectfully,

(b) (6), (b) (4), (b) (7)

(b) (6), (b) (4), (b) (7)

(b) (4), (b) (7)
Office: (b) (6), (b) (4)

(b) (6)

From: Kudwa, Amy
Sent: Thursday, August 26, 2010 7:32 PM
To: 'Beers, Rand'; Reitinger, Philip; McConnell, Bruce; Schaffer, Gregory; Brown, Michael A.
Cc: Denning, John
Subject: WaPo re. DIB pilot

I'm astounded it took this long – (b) (6) (b) (5)

(b) (5)

(b) (6)

From: McDermott, Thomas M
Sent: Monday, May 03, 2010 12:22 PM
To: Schaffer, Gregory; Brown, Michael A.
Cc: Dean, Nicole M; (b) (6) (b) (6)
Subject: Weekly Legal Cyber Meeting

Sirs –

Just to let you know that with both David D. and Doug out of the office today and following (b) (6) departure to FEMA, I am "an army of one" for the day. We can continue with the regularly scheduled 4:00 meeting this afternoon if there are items that you would like to discuss. (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)

(b) (6)

From: (b) (6)
Sent: Monday, October 25, 2010 10:22 AM
To: Brown, Michael A.
Cc: (b) (6)
Subject: ***RADM Brown*** HOT FOR APPROVAL - DoD and DHS Joint Cyber Pilot Plan, Preliminary Version, October 2010 --- 10/20/2010
Attachments: DoDDHS_Joint Cyber Pilot Plan_Preliminary Version_October 2010_DRAFT_ 10202010v10.docx

Importance: High

Sir,

Attached is the DoD and DHS Joint Cyber Pilot Plan, for your approval.

Please note the following comments from Brian Dōne:

(b) (5)

Paul did not get a chance
Thank you,

(b) (6)
Executive Secretariat
Office of Cybersecurity and Communications
U.S. Department of Homeland Security
Office: (b) (6)
BlackBerry: (b) (6)
(b) (6)

Did you know? October is **National Cybersecurity Awareness Month.**
Remember: Cybersecurity is Our Shared Responsibility. For helpful tips you can use to protect yourself, log on today to www.StaySafeOnline.org or www.dhs.gov/cyber.

From: Denning, John
Sent: Wednesday, October 20, 2010 2:20 PM
To: (b) (6)
Cc: CS&C EXEC SEC
Subject: FW: ***Denning*** HOT FOR APPROVAL - DoD and DHS Joint Cyber Pilot Plan, Preliminary Version, October

2010 --- 10/20/2010
Importance: High

Recommend approval

John Denning, Director of External Affairs
Office of Cybersecurity and Communications
Department of Homeland Security
Desk: (b) (6)
Secondary: (b) (6)
Web: www.dhs.gov/cyber

From: Done, Brian
Sent: Wednesday, October 20, 2010 1:35 PM
To: CS&C EXEC SEC
Subject: Request for CS&C ExecSec Review: DoD and DHS Joint Cyber Pilot Plan, Preliminary Version, October 2010 --- 10/20/2010
Importance: High

Sam & (b) (6),

I spoke with RADM Brown this morning. I've made a few (b) (5)

Please send through the CS&C ExecSec process with a focus (b) (5)

(b) (5)

(b) (5)

Please let me know if you have any other questions.

Thanks!

-BKD

Brian K. Dōne
DHS/NPPD/CS&C
M: (b) (6)
E: (b) (6)

CS&C SharePoint Site: (b) (7)(E)
CS&C Enterprise Architecture SharePoint Site: (b) (7)(E)
CS&C External Website: http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm

---

In support of the CS&C mission, how can we most effectively enhance the security, resiliency, and reliability of the nation's cyber and communications infrastructure?

---

*This email message could have been sent quickly from a BlackBerry device, therefore please excuse any clarity, grammar, or spelling mistakes.
*Although I try to keep up with as many emails as possible, if something is time critical, please call the number listed above and/or involve other team members.
*This electronic communication (email / attachments) might have specific use, dissemination, and retention restrictions based on law, executive order, memorandum, policy, guidance, etc.

(b) (6)

From: (b) (6)
Sent: Monday, December 12, 2011 2:56 PM
To: Dean, Nicole M
Cc: Shabat, Matthew; Mesterhazy, Paul; (b) (6)
Subject: *DEAN* OMB Passback Taskers - Various Due Dates
Attachments: NCPS_OMB-MSR_DECFY12v9.pptx

Follow Up Flag: Follow up
Due By: Friday, December 09, 2011 4:00 PM
Flag Status: Flagged

Nicole,

FYI – Budget is working on this but I wanted you to have a copy of it to review. This is due to NPPD this afternoon so an expedited review would be greatly appreciated.

Thank you,
(b) (6)

(b) (6)
NCSD Front Office Executive Secretariat
(b) (6)
U.S. Department of Homeland Security
Office: (b) (6) | BlackBerry: (b) (6)

From: (b) (6)
Sent: Monday, December 12, 2011 12:36 PM
To: (b) (6)
Cc: NCSD Exec Sec; NCSD Budget Exec Sec ; NSD Exec Sec; NSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

(b) (6)

Please find our report attached. Our sincere apologies for the delay.

Thanks,
(b) (6)

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

From: (b) (6)
Sent: Monday, December 12, 2011 10:50 AM
To: (b) (6)
Cc: NCSD Exec Sec; NCSD Budget Exec Sec ; NSD Exec Sec; NSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

(b) (6)

Can I have an ETA on this report?

Thanks,
(b) (6)

(b) (6)
NCSD Front Office Executive Secretariat
(b) (6)
U.S. Department of Homeland Security
Office: (b) (6) | BlackBerry: (b) (6)

From: (b) (6)
Sent: Friday, December 09, 2011 12:50 PM
To: (b) (6)
Cc: NCSD Exec Sec; NCSD Budget Exec Sec ; NSD Exec Sec; NSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

By COB today, we hope.

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

From: (b) (6)
Sent: Friday, December 09, 2011 12:44 PM
To: (b) (6)
Cc: NCSD Exec Sec; NCSD Budget Exec Sec ; NSD Exec Sec; NSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

(b) (6)

May I have an ETA on this report?

Thank you,
(b) (6)

(b) (6)
NCSD Front Office Executive Secretariat
(b) (6)
U.S. Department of Homeland Security
Office: (b) (6) | BlackBerry: (b) (6)

From: (b) (6)
Sent: Wednesday, December 07, 2011 10:34 AM
To: (b) (6)

Cc: NCSD Exec Sec; NCSD Budget Exec Sec ; NSD Exec Sec; NSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

(b) (6)

We will need an extension to Friday on the monthly update taskers. We have a draft of the monthly update ready; however due to scheduling conflicts, our leadership is not available to review until late tomorrow. We will need to submit on Friday to allow us time for leadership review and time for us to incorporate their feedback prior to submitting to NCSD.

Thanks,
(b) (6)

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

From: (b) (6)
Sent: Monday, December 05, 2011 8:50 AM
To: Rock, Lee; (b) (6) USCERT PM; NSD Exec Sec; Menna, Jenny; Hanson, Eric; (b) (6) NSD Budget Exec Sec
Cc: NCSD Exec Sec; NCSD Budget Exec Sec
Subject: OMB Passback Taskers - Various Due Dates

Good morning US-CERT, NSD, & CICPA,

As a result of the OMB FY13 Passback discussions for NPPD, the following taskers must be completed by their prescribed due dates:

(b) (5)

Please reach out to NCSD Budget and Finance with any questions.

Thank you,
(b) (6)

(b) (6)
NCSD Front Office Executive Secretariat
(b) (6)
U.S. Department of Homeland Security
Office: (b) (6) | BlackBerry: (b) (6)

From: (b) (6)
Sent: Thursday, December 01, 2011 3:09 PM
To: (b) (6) NCSD Budget Exec Sec
Subject: RE: OMB Passback Taskers - Various Due Dates

Greetings (b) (6)

For this tasker, please institute the deadlines listed below as the back-to-dates for NCSD Budget/ExecSec. Additionally, please emphasize that it is imperative the taskers are completed by their prescribed due dates:

(b) (5)

Have a great day

(b) (6)
NCSD Office of Budget & Finance
National Cyber Security Division (NCSD)
National Protection and Programs Directorate (NPPD)
U.S. Department of Homeland Security (DHS)

Office: (b) (6)
BlackBerry: (b) (6)
(b) (6)

"Remember you attitude determines your appitude" so just smile!

From: (b) (6)
Sent: Thursday, December 01, 2011 9:57 AM
To: NCSD Budget Exec Sec
Cc: NCSD Exec Sec
Subject: FW: OMB Passback Taskers - Various Due Dates
Importance: High

All,

I received this email yesterday – please reply back with the deadlines you require for this task.

Thank you,
(b) (6)

(b) (6)
NCSD Front Office Executive Secretariat
(b) (6)
U.S. Department of Homeland Security
Office: (b) (6) | BlackBerry: (b) (6)

From: Casapulla, Stephen
Sent: Wednesday, November 30, 2011 4:50 PM
To: NCSD Exec Sec
Cc: CS&C EXEC SEC; Teetz, Lisa; CS&C Budget Exec Sec; Stubbs, Lee; Ward, Linda COS
Subject: OMB Passback Taskers - Various Due Dates
Importance: High

NCSD,
As a result of the OMB FY '13 Passback discussions for NPPD, the following taskers must be completed by their prescribed due dates:

(b) (5)

00267

(b) (5)

[redacted]

If you have any questions, please feel free to contact me or Lisa Teetz, CS&C Budget Director. In your response to these taskers, please send to CS&C ExecSec with a cc' to CS&C Budget ExecSec.

Thank you for your assistance,
Steve

Stephen L. Casapulla
Director - Executive Secretariat
Cybersecurity & Communications
Department of Homeland Security

Office: (b) (6)
E-mail: (b) (6)

(b) (6)

From: Sand, Peter
Sent: Thursday, July 08, 2010 9:21 AM
To: Brown, Michael A.
Cc: (b) (6) (b) (6) (b) (6) (b) (6) Callahan, Mary Ellen; (b) (6); Landesberg, Martha
Subject: [DPIAC/Cyber] DIB Pilot

Sir,

(b) (6), on the subcom, also on ISPAB with (b) (6), sent in the below clip.

Would you mind covering this topic in your opening remarks for next Thirsday's privacy meeting?

I imagine they'd ask:

(b) (5)

Also, Margo Schlanger, DHS CRCL Officer will attend and we blocked a few minutes for her in the opening section.

Thanks,

Pete

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

From: (b) (6) (b) (6)
To: Sand, Peter (b) (6)
Sent: Wed Jul 07 21:42:42 2010
Subject: Fwd: Extension of Einstein III to the Private Sector

Pete --

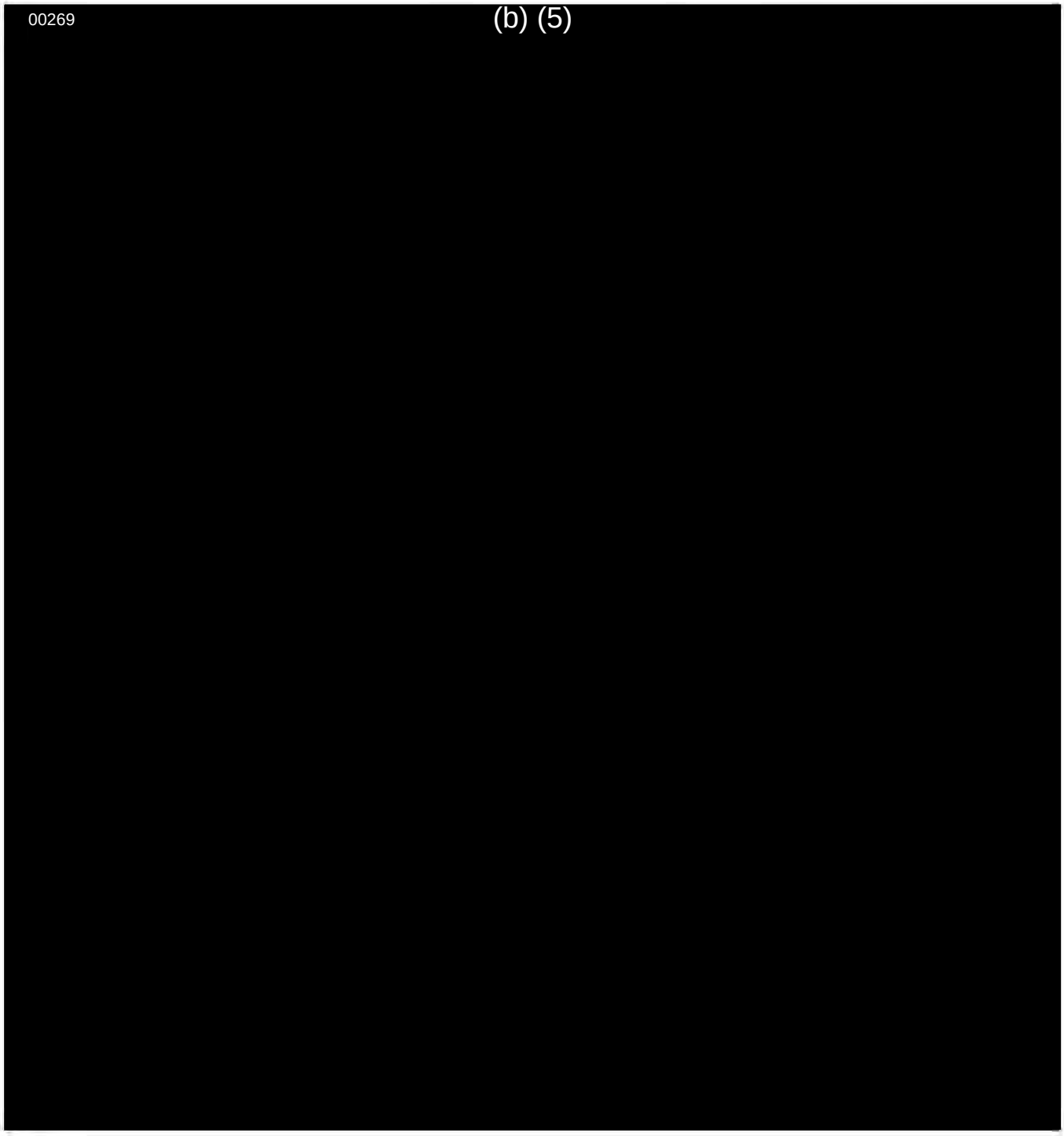
I am inclined (b) (5)

Thanks

To view this email as a web page, go here.

00269

(b) (5)



(b) (6)

From: Sand, Peter
Sent: Saturday, July 17, 2010 7:48 AM
To: Callahan, Mary Ellen; Brown, Michael A.
Cc: John W. Kropf (b) (6) ; Landesberg, Martha
Subject: [DPIAC/Cyber] proposed summary for recent meeting

MEC, Sir,

What if we sent (b) (5)
(b) (5) Here's a draft for your review:

(b) (5)

Pete

(b) (6)

From: Dean, Nicole M
Sent: Thursday, December 01, 2011 9:54 AM
To: Goode, Brendan; (b) (6) 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) Jacobs, Michael; Arnold, Patrick; Allen, Brian; Falkenstein, Cindy; Andrew, Emily
Subject: JCSP Transition Activities - banner meeting

Tom,
Can you provide an overview to the group of the discussion last night please on the DOD/DHS/DOJ con call?

Nicole

(b) (6)

From: Isola, Meredith
Sent: Tuesday, March 22, 2011 6:52 AM
To: NPPD Morning Headlines
Subject: Morning Headines - March 22, 2011
Attachments: Morning Headlines_Mar 22 2011.doc

See full text of articles in the attached document.

Analysis: Face of Federal IT Security Leadership

Why DHS, Not White House, Took Lead on RSA Breach Response

By Eric Chabrow
GovInfoSecurity.com

Pondering government cybersecurity leadership, first thoughts might go to the White House and the office of Cybersecurity Coordinator Howard Schmidt. But the voice of IT security in the Obama administration often seems to be the Department of Homeland Security, not the White House. And, the government's face on cybersecurity matters could be that of Philip Reitinger, deputy undersecretary for the National Protection and Programs Directorate, DHS's highest ranking cybersecurity executive.

When RSA announced last week that it was under a sophisticated attack targeting its SecurID products, inquiries to Schmidt's White House office, the Pentagon and the National Security Agency about how the federal government is responding to the virtual assault and what impact it was having on government IT security were referred to DHS. DHS initially didn't have a response. By late Friday, DHS issued a 119-word statement that provided scant details but said the government was working with RSA on the problem and that federal agencies have been notified about the breach that involved the two-factor authentication product (see *DHS Responds to RSA SecurID Attack*).

DHS provided the government's reaction to the RSA breach because Homeland Security is responsible for operational responses to cyber incidents in civilian agencies and key private-sector IT systems, said Karen Evans, who served as the de facto federal chief information officer in the Bush White House. The White House, she said, is focused on cybersecurity strategy.

(The NSA, a Defense Department agency, serves as the primary IT security agency for DoD and the intelligence community, while providing its technical expertise to civilian agencies through DHS. The NSA director also serves as commander of the U.S. Cyber Command.)

"It is DHS's job to do the daily work of protecting the cybersecurity of the non-DoD country," said Alan Paller, research director at the SANS Institute, a not-for-profit cybersecurity educational organization. "A more public role by the White House would not be more effective and would probably be counterproductive." Counterproductive? "It would undermine DHS effectiveness by implying that a DHS response is insufficient," Paller explained. "The White House weakens DHS if it makes the press believe a DHS response is insufficient."

Article link: http://www.govinfosecurity.com/articles.php?art_id=3454

***

Security Experts, DHS, Lawmakers React To RSA Hack

By Dan Kaplan
SC Magazine

Five days after RSA announced that its systems were breached by a sophisticated attack, details remain scant about how customers of its SecurID two-factor authentication products may be affected.

Still, that hasn't stopped many in the security community from speculating.

Here are latest details emerging:

- The U.S. Department of Homeland Security (DHS) has joined the investigation into the compromise. "Working with RSA, we are leveraging the technical, investigative and mitigation expertise of U.S. government agencies to address this issue," Amy Kudwa, a DHS spokeswoman, told SCMagazineUS.com. "We take threats to our cyber infrastructure as seriously as we take threats to our conventional, physical infrastructure. DHS is also in the process of distributing similar information to our critical infrastructure partners."

- Federal lawmakers also are weighing in. Sen. Susan Collins, R-Maine, chairwoman of the Homeland Security Committee, said in a statement that the "need to pass comprehensive cybersecurity legislation is more urgent than ever" following disclosure of the breach. She said Congress needs to mandate how private and public sector players collaborate to deter attacks.

Article link: http://www.scmagazineus.com/security-experts-dhs-lawmakers-react-to-rsa-hack/article/198832/

***

RSA Security Breach Compromised Federal Network ID Tool

By Aliya Sternstein
NextGov.com

A product many federal employees use to log on to computers and networks should be regarded as compromised, due to the infiltration of key information about the application during a cyberattack against manufacturer RSA, some security experts said.

The Homeland Security Department -- the civilian agency that oversees commercial and government cybersecurity -- has relayed mitigation procedures to federal agencies that have installed RSA's SecurID tools, the department announced on Friday. A DHS official on Monday said the government is not recommending that agencies replace their SecurID products. The department is helping RSA and clients who control critical infrastructure deal with the threat to the devices, which are a single point of failure in the computer security ecosystem, according to some industry observers.

Agencies "should consider [the ID tools] breached," said Tom Kellermann, a former World Bank computer specialist and now an executive at Core Security Technologies, a firm that lawfully penetrates its clients' systems to identify network weaknesses.

SecurID, which verifies the identities of authorized users, consists of a token -- a portable physical object such as a smart card or USB drive that controls access to a system. The device displays a continuously changing code that the user enters, in conjunction with a personal identification number, or PIN, to log into a network through a process known as two-factor authentication.

RSA officials said agencies should not stop using the SecurID products because the information the culprit gleaned is insufficient to launch an attack by itself. "To the best of our knowledge, whoever attacked RSA has certain information related to the RSA SecurID solution, but not enough to complete a successful attack without obtaining additional information that is only held by our customers," an RSA spokesman said in an e-mail.

Article link: http://www.nextgov.com/nextgov/ng_20110321_6511.php?oref=topstory

***

U.S. May Strengthen Identity Verification System For Workers

By Shankar Vedantam
The Washington Post

The federal government is exploring the possibility of using a credit rating giant like Equifax to verify the identity of American workers, a move that could make it far more difficult for undocumented immigrants to get work using stolen Social Security numbers.

The plan by the Department of Homeland Security, which is still preliminary and would probably require congressional approval, could have far-reaching consequences. The government already allows employers to check the legal status of employees using a system known as E-Verify, but hundreds of thousands of undocumented immigrants beat the system by using stolen Social Security numbers.

If workers had to use the verification systems in place to apply for a mortgage or a bank account, they would not only have to present a Social Security number to an employer, but also answer questions about their personal history and financial background to establish their identity.

Article link: http://www.washingtonpost.com/local/us-may-strengthen-identity-verification-system-for-workers/2011/03/21/ABH8Si8_story.html

***

AP Enterprise: Terror Suspects Seek To Clear Names

By Chris Hawley and John Curran
The Associated Press

As the U.S. ramps up efforts to root out homegrown terrorism, hundreds of people who have fallen under suspicion are in a state of limbo: Many say they have been singled out unfairly for scrutiny but have been neither charged nor cleared.

Some of them, mostly Muslims, have spent weeks in jail; others find it impossible to travel freely. Some say they have had their reputations destroyed by the news coverage. Many were questioned or tracked, and say they felt violated and fearful.

Lawsuits filed by suspects since 2006 have pried millions of dollars in settlements from the government. The U.S. Supreme Court this month heard one of the most serious challenges yet, the case of a Kansas man who claims his detention as a "material witness" destroyed his marriage and his career.

Many plaintiffs say they recognize the security challenges the government faces after Sept. 11; but in many cases, they complain, the government refuses to reveal why someone has attracted attention. Without that information, they argue, it is impossible to clear their names.

Article link:
http://hosted.ap.org/dynamic/stories/U/US_TERROR_UNDER_SUSPICION?SITE=VANOV&SECTION=HOME&TEMPLATE=DEFAULT

***

Online Fraud Hotspots Named

By John E Dunn (Techworld.com)
PC World

Online fraud against U.K. merchants is at levels that have forced many to refuse orders from certain countries, with Nigeria, Ghana, and the U.S. heading the list, a new e-commerce report has found.

According to payment company CyberSource's annual fraud analysis of 200 companies, 55 percent of U.K. companies questioned refused to ship to Nigeria at all, ahead of Ghana on 34 percent, and, surprisingly, the U.S. on 25 percent.

Of digital-only companies (i.e, those shipping downloadable goods as opposed to physical ones) Nigeria again headed the blacklist, with 47 avoiding it ahead of Vietnam, China, and South Korea on 29 percent each, and the U.S. on 24 percent.

The average fraud rate was now 1.6 percent of orders, down from 1.8 percent in 2009, with digital retailers suffering the highest rates overall. Rejection rates for online sales are now 5 percent.

Article link: http://www.pcworld.com/article/222299/online_fraud_hotspots_named.html

***

Australia Should Appoint Cyber Security Czar

Yahoo!7, ninemsn and Microsoft Australia say cyber security czar or ombudsman could better coordinate government and industry activities

By Tim Lohman
Computerworld

The creation of an Australian cyber security czar or ombudsman is needed, but would be of limited use in the promotion of greater online security, a Senate inquiry has heard.

Ninemsn's compliance, regulatory and corporate affairs director, Jennifer Duxbury, told a committee hearing into cyber safety that there were already government agencies responsible for cyber safety issues, such as the Australian Federal Police and the Australian Communications and Media Authority.

"If there was to be an [cyber safety] ombudsman, one of the challenges would be the fact that a lot of cyber safety issues can be offshore, so there is a jurisdictional challenge there as to how an ombudsman would actually deal with complaints which deal with, for example, inappropriate offshore material," she said.

Microsoft Australia chief security advisor, Stuart Strathdee, said a lot of work was already being carried out on cyber safety but an ombudsman or czar could contribute to greater direction and coordination of existing efforts.

Article link: http://www.computerworld.com.au/article/380545/australia_should_appoint_cyber_security_czar/

***

Cyber Command Pursues 'Defensible' IT Architecture

The Defense agency's top executive outlines a series of initiatives, including development of a hardened IT architecture that incorporates cloud computing and thin clients.

By Elizabeth Montalbano
InformationWeek

Gen. Keith Alexander has outlined a series of next steps to be pursued by the six-month-old U.S. Cyber Command, including development of a "defensible architecture" that's better suited for the latest generation of cyber threats.

Alexander is director of the National Security Agency and commander of U.S. Cyber Command, which operates out of Fort Meade in Maryland and reports to U.S. Strategic Command within the Department of Defense. Last year, he painted a dire picture of the threats to DoD networks, revealing they're subject to 250,000 probes every hour. Last week, in testimony to the House Armed Services Committee, he reiterated the urgency of securing DoD networks.

The threats continue to mature and, while no major attack has happened so far, the United States must be prepared, Alexander said. "We are collectively vulnerable to an array of threats ranging from network instability to criminal and terrorist activities to state-sponsored capabilities and actions that are progressing from exploitation to disruption to destruction," he said.

U.S. Cyber Command became operational in October. Alexander outlined several challenges facing his organization, including the need to prevent a "cyber 9/11" type of attack on critical infrastructure.

Article link:
http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229400008

***

Government Eyeing Security Technology To Prevent Another Wikileaks

The Intelligence Community is trying to find a "sweet spot" between sharing intelligence information while preventing unauthorized access to that data by people who might misuse it, an official told Congress.

By Elizabeth Montalbano
InformationWeek

U.S. intelligence agencies are eyeing the use of new security technology to help prevent another insider data breach like the one that caused the Wikileaks international scandal last year.

Testifying before the Senate Homeland Security and Governmental Affairs Committee earlier this month, Corin Stone, the Intelligence Community's (IC) information sharing executive, said that striking a balance between sharing intelligence information while still protecting data against insider threats is a persistent problem within the community, and one that it will use technology to solve.

The Intelligence Community is a coalition of 17 U.S. intelligence agencies and departments -- including the Central Intelligence Agency, the Federal Bureau of Investigations, the Office of National Intelligence, and the Defense Intelligence Agency -- that perform intelligence operations.

Article link:
http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229301353

***

Blue-Ribbon Panel Calls for Airport Screening Reforms

By Phil Leggiere
Homeland Security Today

The current aviation security system is discouraging Americans from flying and contributing to a decline in productivity among those who do fly, according to a report put together by a blue ribbon panel.

The report, *A Better Way : Building a World Class System of Aviation Security*, which was prepared under the auspices of the US Travel Association, begins by asking: "Is today's security screening system the most cost effective and efficient that the United States can possibly produce?"

Its answer: "No. The country that put a man on the moon, invented the Internet and creates daily innovations in manufacturing can and must do better."

The panel's members included Tom Ridge, former Secretary of the Department of Homeland Security and CEO of Ridge Global; former Ranking Democratic Member of the House Homeland Security Committee Jim Turner, currently Partner at Arnold & Porter; and Rick "Ozzie" Nelson, director of the Homeland Security and Counterterrorism Program at the Center for Strategic & International Studies.

Article link: http://www.hstoday.us/industry-news/general/single-article/blue-ribbon-panel-calls-for-airport-screening-reforms/300e0f669d4cdcf07e8b3b18db6297c1.html

***

Homeland Security Offers Tool To Curb Errors In Work Eligibility

By George A. Warner
NextGov.com

Workers will have a new electronic means to help prevent the government from mislabeling them as ineligible for U.S. employment, Homeland Security Secretary Janet Napolitano announced on Monday.

"Beginning today, for the first time, individuals in five states and the District of Columbia will be able to check their own employment eligibility status before seeking a job," Napolitano said at a news conference announcing the pilot program. "This new service is voluntary, is fast, is free and, importantly, is secure."

Officials at U.S. Citizenship and Immigration Services, a division of the Homeland Security Department, hope the program will cut back on the number of documented workers whose status is wrongly questioned because of database errors in the E-Verify work eligibility system during the hiring process.
The Self Check program provides "clear instructions in both English and Spanish on how the user can correct his or her records," USCIS Director Alejandro Mayorkas said at the press conference.

Despite its limited availability, USCIS sees the program expanding soon. The agency plans to implement the program nationwide by the end of 2012, but a USCIS fact sheet warned that implementation plans were contingent on "personnel and budgetary" resources. USCIS expects about 1 million people will self-query their employment eligibility status in the next year, and that figure could reach up to 8 million checks per year once the program is available nationwide.

Article link: http://www.nextgov.com/nextgov/ng_20110321_5655.php

***

Senators Start Talks On Larger Cybersecurity Bill

Senior Senate staff members working on the issue of cybersecurity and how to address it in law

By Matthew Weigelt
Federal Computer Week

Senators are beginning talks on pushing cybersecurity legislation, hoping for a successful run this time.

Top Senate staff members have been in discussions for several weeks, working to parse language from at least two separate cybersecurity bills that were introduced but not passed in the previous Congress, while senators have just joined the talks, according to Molly Wilkinson, counsel for the Senate Homeland Security and Governmental Affairs Committee.

"Senior leadership in the Senate is working toward the issue of cybersecurity and how to address it," Wilkinson said March 17 during a panel discussion at the Coalition for Government Procurement's Spring Conference. However, she added that the talks were in the beginning stages.

Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine), the chairman and ranking member, respectively, of the Senate Homeland Security and Governmental Affairs Committee, introduced the Protecting Cyberspace as a National Asset Act of 2010 last June. The committee approved the legislation by voice vote in December, but it died in the full Senate.

Article link: http://fcw.com/articles/2011/03/21/cybersecurity-legislation-talks-senate.aspx

***

DIB Active Defense Cybersecurity Pilot Near Start

By David Perera
FierceGovernmentIT

[1]The Defense Department is close to starting a 90-day pilot with the defense industrial base that will test an active defense capability analogous to the Homeland Security Department's Einstein 3 effort, said a top Defense Department official during a House panel March 16.

While testifying before the House Armed Services subcommittee on emerging threats and capabilities, James Miller, the principal deputy undersecretary of defense for policy, said the Pentagon has already approached defense contractors and Internet service providers about participation the pilot. In all, 30 firms will likely participate in the pilot, said Gen. Keith Alexander, the head of Cyber Command and the National Security Agency, who also testified at the hearing.

"By way of analogue, it's looking to, for a part of the .com, to bring what Einstein 3 is supposed to bring the .gov," Miller said.

The DoD has already started a pilot testing greater information sharing with the private sector, Miller said. "It's been a two-way street, it's been very effective, and we're looking to continue and grow that," he added.

Article link: http://www.fiercegovernmentit.com/story/dib-active-defense-cybersecurity-pilot-near-start/2011-03-20

***

How Stuxnet Changes The Security Game

New attacks could cross the 'air gap' to systems not connected to the Internet

By (ISC)2 Government Advisory Board Executive Writers Bureau – *COMMENTARY*
Government Computer News

In November 1988, the first computer worm indiscriminately propagated through 6,000 Unix systems, or roughly 10 percent of the computer systems on the Internet. Although developed with innocuous intent, this worm had the ability to duplicate itself repeatedly in a given environment, ultimately causing the affected system to fail.

Roughly 22 years later, the Stuxnet worm emerged as a technological advancement with the potential to cause an unimaginable impact. Many have heralded it as a paradigm shift in the cyber threat landscape because of its precision targeting, as opposed to indiscriminate destruction. Instead of attacking every system it enters, Stuxnet is designed to only subvert specific Supervisory Control and Data Acquisition systems.

While using common operating systems and networking components, SCADA systems have traditionally been air-gapped from the Internet to pre-empt such attacks. In the case of Stuxnet, the worm was able to bridge this gap through targeting specific systems and using removable media.

Given the potential damage this malware advancement is capable of causing, security professionals need to re-evaluate their perceptions of risk and challenge their preconceived notions regarding segmented networks and critical infrastructure.

In order to stay on the cutting edge of threat advancement, security practitioners traditionally have sought the newest tools and techniques that would provide greater insight into how to build and manage secure networks. Tools employed in recent years to maintain that edge include Intrusion Prevention Systems and Data Loss Prevention suites.

However, it is important to consider that a shift in focus from basic security practices to more sophisticated implementations such as IPS or DLP can often allow the "urgent" to overshadow the "fundamental," from both a security posture and budgetary standpoint. There is evidence that, although Stuxnet was designed to circumvent our industry's leading security technology, it might not have been as far-reaching if certain fundamental security controls had been in place.

Article link: http://gcn.com/articles/2011/03/21/commentary-stuxnet-new-threats.aspx

***

FBI Announces Creation of Biometric Database