

Andrew, Emily

From: Sand, Peter
Sent: Friday, March 25, 2011 11:28 AM
To: Callahan, Mary Ellen; John W. Kropf (b) (6) Andrew, Emily
Subject: DIB Pilot Starting and Branded as a DHS program
Attachments: PA DIB Pilot Briefing Card 2011-03-17.doc

Importance: High

MEC,

See below from RADM Brown. I'll find out timing and exactly what DHS's role is - this could be .com traffic going to DHS and DoD.

(b) (5)

Alex Joel asked for a briefing. I haven't heard from (b) (6) - we just found out through Brown yesterday.

I'll let you know more as I learn it and will push back as though we are doing a public PIA.

Pete

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

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

From: Brown, Michael A. RADM
Sent: Thursday, March 24, 2011 3:03 PM
To: McNeely, James; Sand, Peter
Cc: Delaney, David; McDermott, Thomas M; (b) (6); Dean, Nicole M; (b) (6)
Subject: FW: PA DIB Pilot Briefing Card 2011-03-17.doc

Team,

(b) (5)

v/r,

MAB

Mike Brown
RADM, USN
Director, Cybersecurity Coordination
National Protection & Programs Directorate Department of Homeland Security
(b) (6) Fort Meade)
(b) (6) (Arlington)

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

From: Kudwa, Amy
Sent: Friday, March 18, 2011 1:35 PM
To: McConnell, Bruce; Brown, Michael A. RADM; Denning, John; (b) (6) (b) (6)
Subject: FW: PA DIB Pilot Briefing Card 2011-03-17.doc

With the caveat that I know everyone is stretched very thin right now, I received these DIB pilot TPs from DoD OPA this morning and they're seeking our input.

In speaking with (b) (6) they're not really getting incoming on this, but want to have something in the can for future use. She understands our operational posture at present, and so agreed that our getting back to her on Monday was fine. Can we internally aim for 10 a.m. Monday?

Thanks,
Amy

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

From: (b) (6) LtCol OSD PA (b) (6)
Sent: Friday, March 18, 2011 11:32 AM
To: 'Kudwa, Amy'
Subject: PA DIB Pilot Briefing Card 2011-03-17.doc

Amy,

As discussed yesterday, attached is DoD's DIB Opt In Pilot briefing card. The messages come from the coordinated communication plan that you all coordinated on, so there is nothing new.

V/r.. (b) (6)

Andrew, Emily

From: Sand, Peter
Sent: Tuesday, April 26, 2011 5:42 PM
To: Brown, Michael A. RADM; Callahan, Mary Ellen
Cc: (b) (6); (b) (6); McNeely, James; (b) (6); Leckey, Eric; Andrew, Emily
Subject: Fw: DIB Pilot PIA status?

Update:

- Mike R is working on a PIA: maybe a draft by next week.
- we can't get an early draft - too many people working on it, too many sensitivities
- working on getting an NSA brief

Unless someone else has another way in, looks like we'll see the PIA when it publishes.

Pete

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

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

From: Reheuser, Michael E SES OSD ODAM/DPCLO (b) (6)
Sent: Tuesday, April 26, 2011 04:22 PM
To: (b) (6); (b) (6)
Subject: Re: DIB Pilot PIA status?

Pete

I am out tomorrow but will check with nsa on Th to see where things are.
Can't do an early view of the pia. Its not mine and there are too many sensitivities surrounding this program to send out at this time. Sorry.

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

From: Sand, Peter (b) (6)
Sent: Tuesday, April 26, 2011 03:50 PM
To: Reheuser, Michael E SES OSD ODAM/DPCLO
Subject: RE: DIB Pilot PIA status?

Thanks, Mike.

No - haven't heard anything yet from NSA. I can reach out through our channels - or is there's someone you recommend we ask?

We've started working on the PIA for E3 - I'd be curious how the two PIAs read together (or maybe the 3 PIAs: our Initiative 3 Exercise PIA, your DIB Pilot PIA, and our E3 PIA).

If there's a way we could get an early reader's copy, that'd be really helpful.

Pete

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

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

From: Reheuser, Michael E SES OSD ODAM/DPCLO (b) (6)
Sent: Tuesday, April 26, 2011 2:08 PM
To: Sand, Peter
Subject: RE: DIB Pilot PIA status?

Pete
We are getting close, but do not yet have the final product.
We have another call tomorrow afternoon. My guess is that we will have something by the end of next week, but with so many cooks in the kitchen, its hard to know what might throw us off.

Has NSA reached out to you about getting a briefing?
They told me that they would but I haven't heard anything yet.

Thanks.

Mike

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

From: Sand, Peter (b) (6)
Sent: Tuesday, April 26, 2011 1:55 PM
To: Reheuser, Michael E SES OSD ODAM/DPCLO
Subject: DIB Pilot PIA status?

Mike,

Has there been any movement yet on the PIA for the pilot? Anything we 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

Andrew, Emily

From: Brown, Michael A. RADM
Sent: Wednesday, May 11, 2011 2:07 PM
To: Sand, Peter; Callahan, Mary Ellen; Andrew, Emily
Cc: (b) (6); (b) (6); McNeely, James; (b) (6); Leckey, Eric; (b) (6)
Subject: Re: [priv-tech update] DIB Pilot - live, no PIA

Pete,

Roger all. Thanks.

Vr,
MAB

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

From: Sand, Peter
Sent: Wednesday, May 11, 2011 10:49 AM
To: Callahan, Mary Ellen; Brown, Michael A. RADM; Andrew, Emily
Cc: (b) (6); Natalie M. Evans; (b) (6); (b) (6); McNeely, James; Rebecca J. Richards; (b) (6); (b) (6); Leckey, Eric; (b) (6)
Subject: [priv-tech update] DIB Pilot - live, no PIA

MEC, Admiral, Emily,

See below update. DIB did start, PIA still in the works. Hopefully we'll get a copy as soon as it's final.

Pete

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

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

From: Reheuser, Michael E SES OSD ODAM/DPCLO (b) (6)
Sent: Wednesday, May 11, 2011 10:40 AM
To: 'Sand, Peter'
Subject: RE: DIB Pilot PIA status?

Pete
Pilot did start, no PIA yet. Its still working through our DoD processes. Lots of cooks in the kitchen.
Will let you know as soon as we have it final.

Thanks.

Mike

Michael E. Reheuser

00827

Director
Defense Privacy and Civil Liberties Office
1901 South Bell Street, Suite 920
Arlington, VA 22202-4512

(b) (6)

(b) (6)

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

From: Sand, Peter (b) (6)
Sent: Wednesday, May 11, 2011 10:06 AM
To: Reheuser, Michael E SES OSD ODAM/DPCLC
Subject: RE: DIB Pilot PIA status?

Mike,

I heard a rumor that the DIB Pilot started? Do you know if that's true and if it means there's a PIA we could look at?

We're still doing prep work for our EINSTEIN 3 PIA - no draft yet.

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

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

From: Reheuser, Michael E SES OSD ODAM/DPCLC (b) (6)
Sent: Tuesday, April 26, 2011 4:23 PM
To: (b) (6)
Subject: Re: DIB Pilot PIA status?

Pete

I am out tomorrow but will check with nsa on Th to see where things are.

Can't do an early view of the pia. Its not mine and there are too many sensitivities surrounding this program to send out at this time. Sorry.

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

From: Sand, Peter (b) (6)
Sent: Tuesday, April 26, 2011 03:50 PM
To: Reheuser, Michael E SES OSD ODAM/DPCLC
Subject: RE: DIB Pilot PIA status?

Thanks, Mike.

No - haven't heard anything yet from NSA. I can reach out through our channels - or is there's someone you recommend we ask?

00828

We've started working on the PIA for E3 - I'd be curious how the two PIAs read together (or maybe the 3 PIAs: our Initiative 3 Exercise PIA, your DIB Pilot PIA, and our E3 PIA).

If there's a way we could get an early reader's copy, that'd be really helpful.

Pete

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

voice: (b) (6) pager: (b) (6) (b) (6) www.dhs.gov/privacy

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

From: Reheuser, Michael E SES OSD ODAM/DPCL0 (b) (6)
Sent: Tuesday, April 26, 2011 2:08 PM
To: Sand, Peter
Subject: RE: DIB Pilot PIA status?

Pete

We are getting close, but do not yet have the final product. We have another call tomorrow afternoon. My guess is that we will have something by the end of next week, but with so many cooks in the kitchen, its hard to know what might throw us off.

Has NSA reached out to you about getting a briefing? They told me that they would but I haven't heard anything yet.

Thanks.

Mike

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

From: Sand, Peter (b) (6)
Sent: Tuesday, April 26, 2011 1:55 PM
To: Reheuser, Michael E SES OSD ODAM/DPCL0
Subject: DIB Pilot PIA status?

Mike,

Has there been any movement yet on the PIA for the pilot? Anything we can help with?

Pete

Peter E. Sand, J.D., CIPP/G/IT

00829

Director of Privacy Technology

Department of Homeland Security

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

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

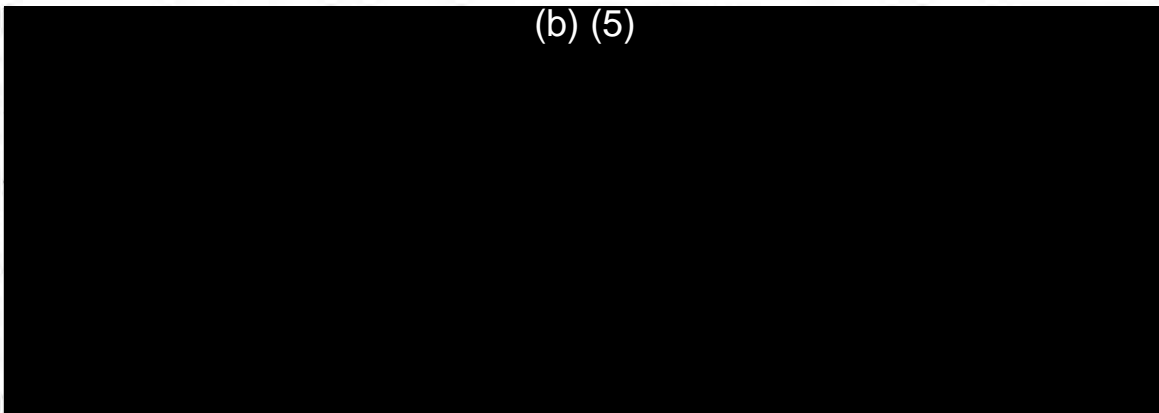
From: [Andrew, Emily](#)
To: [Lockett, Vania](#); [Falkenstein, Cindy](#)
Subject: FW: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot
Date: Tuesday, June 07, 2011 2:17:08 PM
Attachments: [PA DIB Pilot Briefing Card 2011-03-17.doc](#)

[More on DIB.](#)

From: Sand, Peter
Sent: Tuesday, June 07, 2011 12:44 PM
To: Andrew, Emily
Subject: RE: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Emily,

(b) (5)



There's a guy inside CS&C: Brian Done (b) (6) ("DOH-n" like "Dome") who has a great handle on the big stuff. He might be worth chatting with.

FYI, There's a call today at 4 that MEC's joining.

Pete

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

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

From: Andrew, Emily
Sent: Tuesday, June 07, 2011 12:19 PM
To: Sand, Peter
Subject: RE: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Pete - I'm trying to get up to speed on the DIB initiative.

1. Who are some of the DIB companies?
2. How is DHS involved?

It appears that DOD is doing a lot of the same things we (US-CERT) are doing with private sector companies.

Thanks
Emily

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

From: Sand, Peter
Sent: Tuesday, June 07, 2011 7:18 AM
To: Andrew, Emily; Callahan, Mary Ellen
Subject: RE: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Here 'ya go.

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

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

From: Andrew, Emily
Sent: Tuesday, June 07, 2011 7:13 AM
To: Callahan, Mary Ellen
Cc: Sand, Peter
Subject: RE: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Mary Ellen - thanks again for including me. Can you forward the draft PIA when you have a moment?

Emily

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

From: Callahan, Mary Ellen
Sent: Monday, June 06, 2011 6:30 PM
To: McConnell, Bruce
Cc: McDermott, Thomas M; Parkinson, Deborah; (b) (6) Sand, Peter; Andrew, Emily
Subject: Re: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Sure, if you think it would be useful. I will join the call tomorrow as well. Mec.

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

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

From: McConnell, Bruce
Sent: Monday, June 06, 2011 06:28 PM
To: Callahan, Mary Ellen
Cc: McDermott, Thomas M; Parkinson, Deborah; (b) (6) Sand, Peter; Andrew, Emily
Subject: Re: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

This most helpful. I am happy to send it on to OSD. Is that ok with you?

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

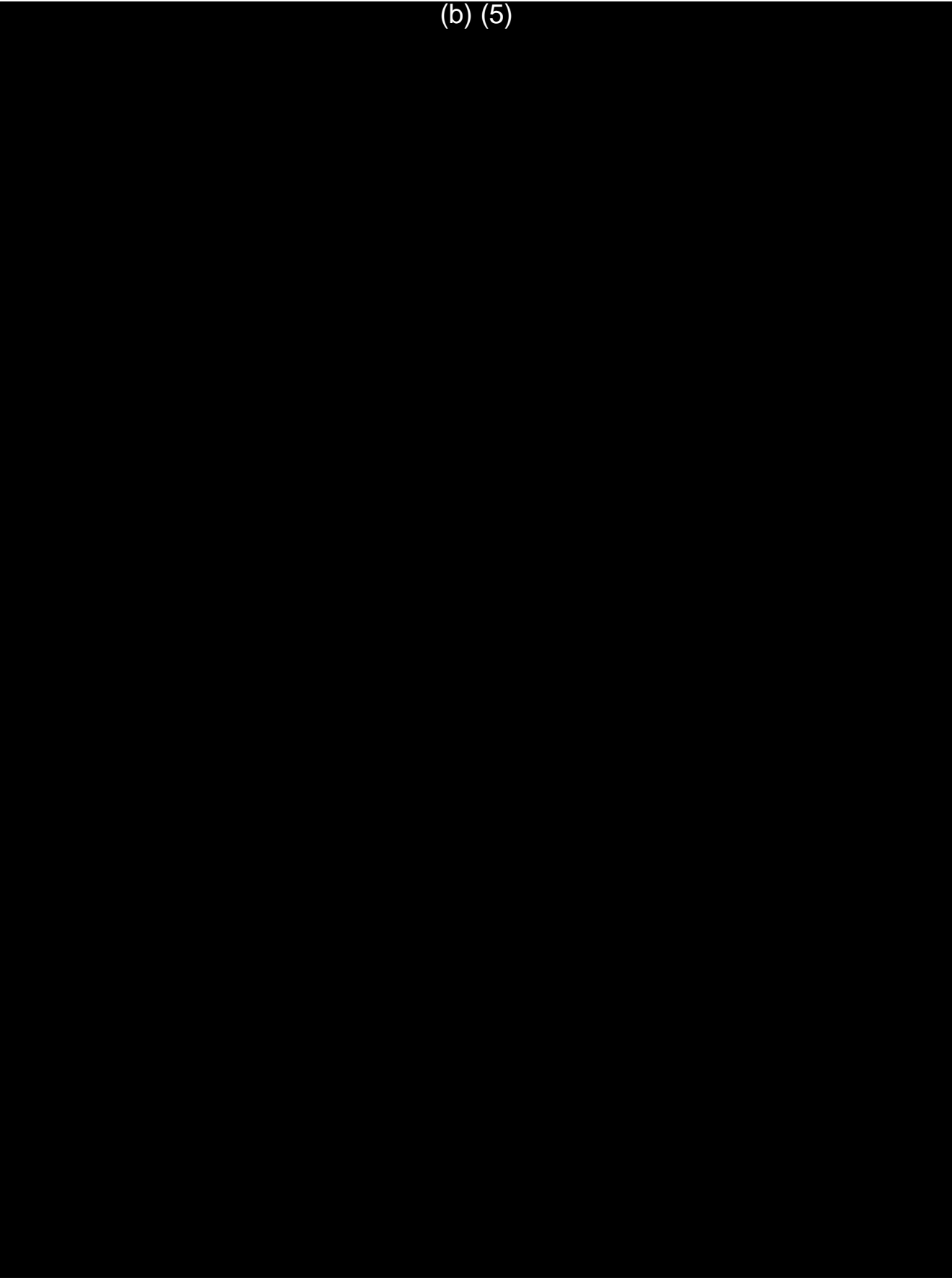
From: Callahan, Mary Ellen
Sent: Monday, June 06, 2011 05:13 PM
To: McConnell, Bruce
Cc: McDermott, Thomas M; Parkinson, Deborah; Callahan, Mary Ellen
(b) (6) Sand, Peter; Andrew, Emily
Subject: RE: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

PREDECISIONAL
DRAFT
DELIBERATIVE

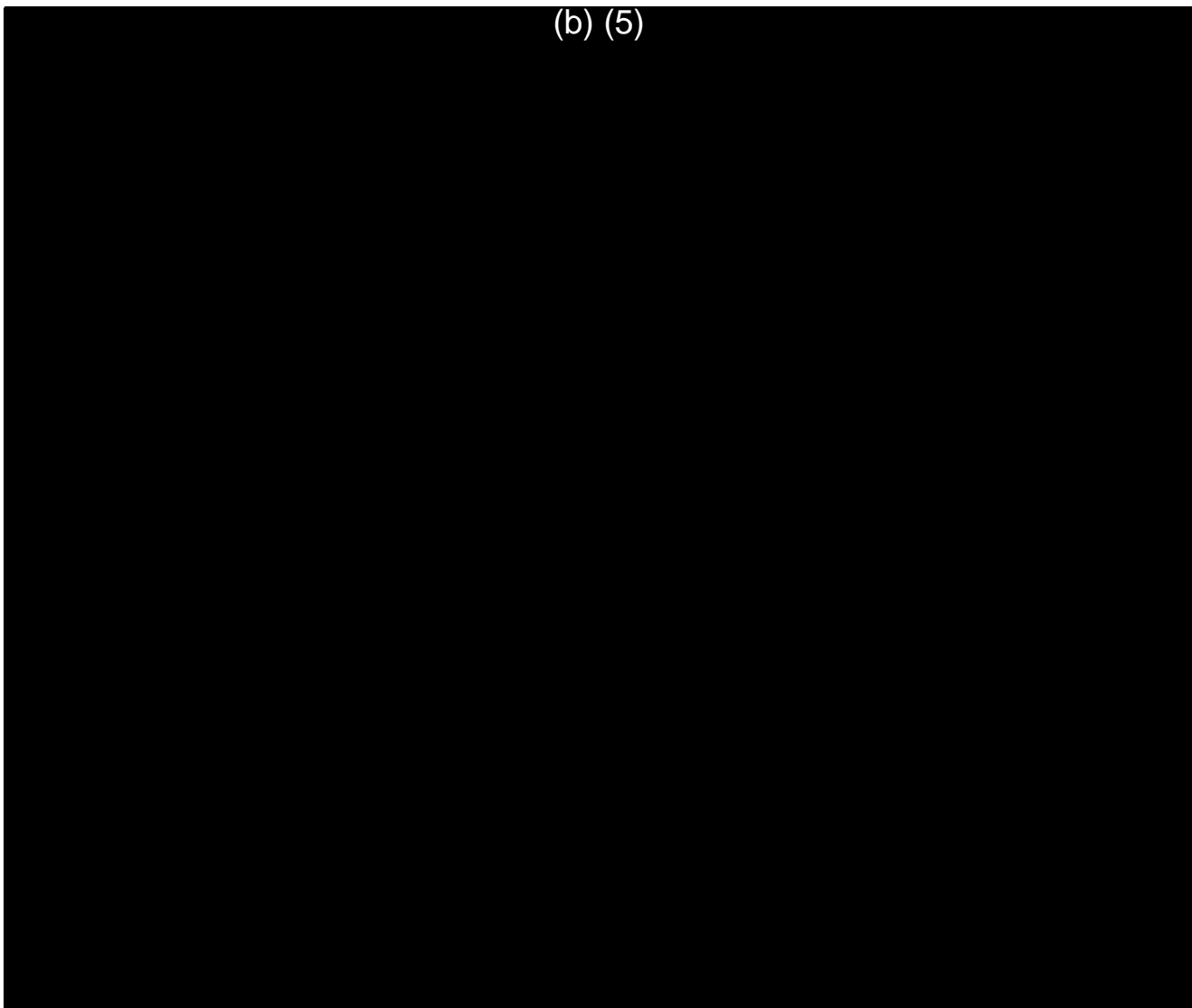
Hi, Bruce,

(b) (5)

(b) (5)



(b) (5)



Best,
Mary Ellen

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

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

From: McConnell, Bruce
Sent: Thursday, June 02, 2011 7:41 PM
To: Callahan, Mary Ellen
Cc: McDermott, Thomas M; Parkinson, Deborah
Subject: Fw: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

Thoughts welcome.

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

From: McDermott, Thomas M [REDACTED] (b) (6)
Sent: Thursday, June 02, 2011 04:57 PM
To: McConnell, Bruce [REDACTED] (b) (6); Parkinson, Deborah [REDACTED] (b) (6)
Subject: FW: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

[REDACTED] (b) (5)

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

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

From: [REDACTED] (b) (6) DoD OGC [REDACTED] (b) (6)
Sent: Thursday, June 02, 2011 4:51 PM
To: Chipman, Jason (SMO); [REDACTED] (b) (6), [REDACTED] (b) (7)(C) (USDoJ); [REDACTED] (b) (6) (NSD) (SMO);
'Delaney, David'; 'McDermott, Thomas M'
Subject: FW: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

FYI/SA - I just realized that you guys were not on this email list when I sent this out.

[REDACTED] (b) (6)
Associate General Counsel
DoD Office of the General Counsel

Direct: (b) (6)
(b) (6)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

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

From: (b) (6) DoD OGC
Sent: Friday, May 27, 2011 2:50 PM
To: (b) (6) Butler, Robert J SES OSD POLICY
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6)
Schleien, Steven, SES, OSD-POLICY; (b) (6) C CIV OSD POLICY; (b)(3)-P.L. 86-36
(b) (6) DISL NII/DoD-CIO; Guissanie, Gary, SES, NII/DoD-CIO; (b) (6)
Mr, DoD OGC; Reheuser, Michael E SES OSD ODAM/DPCLO; (b) (6)
DoD OGC; (b)(3)-P.L. 86-36
Subject: Draft Privacy Impact Assessment (PIA) for DIB CS/IA and Opt-in Pilot

(b) (5)

Looking forward to your review, comments, edits.

Have a great, long, SAFE holiday weekend!

(b) (6)

(b) (6)
Associate General Counsel
DoD Office of the General Counsel
Direct: (b) (6)
(b) (6)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further

without approval from the Office of the DoD General Counsel.

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

From: (b) (6) (b) (6)
Sent: Tuesday, May 24, 2011 8:20 PM
To: Butler, Robert J SES OSD POLICY; (b) (6) DoD OGC
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY; (b) (6) C CIV OSD POLICY
Subject: RE: Privacy Impact Assessment

Thanks for the update - we look forward to receiving the draft by Thursday.

Best,

(b) (6)

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

From: Butler, Robert J SES OSD POLICY (b) (6)
Sent: Tuesday, May 24, 2011 5:50 PM
To: (b) (6) DoD OGC; (b) (6)
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY; (b) (6) C CIV OSD POLICY
Subject: RE: Privacy Impact Assessment

Thanks (b) (6)

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

From: (b) (6) DoD OGC
Sent: Tuesday, May 24, 2011 5:30 PM
To: Butler, Robert J SES OSD POLICY; (b) (6)
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY; (b) (6) C CIV OSD POLICY
Subject: RE: Privacy Impact Assessment

(b) (5)

point.

(b) (6)
Associate General Counsel
DoD Office of the General Counsel
Direct: (b) (6)
(b) (6)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

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

From: Butler, Robert J SES OSD POLICY
Sent: Tuesday, May 24, 2011 2:36 PM
To: (b) (6)
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY; (b) (6) C CIV OSD POLICY; (b) (6) DoD
OGC
Subject: RE: Privacy Impact Assessment

(b) (6) : (b) (6) and (b) (6) are working ... more from them ... Sincerely, Bob

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

From: (b) (6) (b) (6)
Sent: Tuesday, May 24, 2011 12:55 PM
To: (b) (6) Butler, Robert J SES OSD POLICY
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY
Subject: RE: Privacy Impact Assessment

Hi Bob,

I followed up with (b) (6) and understand you discussed last night and we should have the draft later today.

Best,

(b) (6)

From: (b) (6)
Sent: Tuesday, May 24, 2011 12:44 PM
To: 'Butler, Robert J SES OSD POLICY'
Cc: (b) (6) (b) (6) R.; (b) (6) (b) (6) Schleien,
Steven, SES, OSD-POLICY
Subject: Privacy Impact Assessment

Hi Bob,

Per our discussion at the IPC last week, we anticipated the draft PIA COB yesterday - can you please provide an update?

Best,

(b) (6)

(b) (6)

Director, Cybersecurity

National Security Staff

(b) (6)

Andrew, Emily

From: Sand, Peter
Sent: Monday, November 07, 2011 7:11 PM
To: Callahan, Mary Ellen; (b) (6) Andrew, Emily
Subject: [Fyi] DIB Pilot SORN + Review

MEC - I skimmed the dib pilot pia and it says a sorn IS required.

Asked Mike about it - says not one yet.

CMU prof is going to talk to Mike as well (I'm talking to prof tomorrow am).

Pete

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

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

From: Reheuser, Michael E SES OSD ODAM/DPCL (b) (6)
Sent: Monday, November 07, 2011 08:04 AM
To: Sand, Peter
Subject: RE: DIB Pilot SORN?

Pete
SORN is not completed.
CMU prof is supposed to call me as well. (b) (6) has the details on what they are doing.
Do you have Richard's contact info?

Mike

Michael E. Reheuser
Director
Defense Privacy and Civil Liberties Office
1901 South Bell Street, Suite 920
Arlington, VA 22202-4512
(b) (6)
(b) (6)
www.dpclo.defense.gov

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

From: Sand, Peter (b) (6)
Sent: Friday, November 04, 2011 10:35 AM
To: Reheuser, Michael E SES OSD ODAM/DPCL
Subject: RE: DIB Pilot SORN?

Mike,

I just noticed the DIB pilot says a SORN is required... is it posted somewhere?

00841

Also, I received a request to talk with a CMU professor as part of an independent study for the DIB pilot- do you have any background on it?

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: [McDermott, Thomas M](#)
To: [Falkenstein, Cindy](#); [Andrew, Emily](#)
Subject: Fw: Discussion Qs re monitoring & consent for DIB OPT-In Pilot Meeting, 9 Dec 2011, 0900-1200
Date: Wednesday, December 07, 2011 6:04:01 PM
Attachments: [Survey-Discussion-Notice-Consent-Prx_draft4_07dec11.docx](#)
Importance: High

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

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

From: McDermott, Thomas M
Sent: Wednesday, December 07, 2011 05:08 PM
To: Dean, Nicole M; Goode, Brendan
Subject: FW: Discussion Qs re monitoring & consent for DIB OPT-In Pilot Meeting, 9 Dec 2011, 0900-1200

Discussion items for Friday. Can one of you forward to (b)(6)-P.L. 86-36 I can't find his unclassified address.

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)

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

From: (b) (6) DoD OGC (b) (6)
Sent: Wednesday, December 07, 2011 9:52 AM
To: McDermott, Thomas M; Delaney, David; (b) (6), (b) (7)(C) (b) (6) (NSD) (JMD); Anderson, Trisha (JMD); (b) (6) (b) (6)
(b) (6)
Cc: (b) (6) Mr, DoD OGC; (b)(3)-P.L. 86-36; (b) (6) (b)(6)-P.L. 86-36 Reheuser, Michael E SES OSD ODAM/DPCLO; (b) (6) DoD OGC; (b) (6) DoD OGC; Hale, Richard A SES DoD CIO; Rosenbach, Eric B SES OSD POLICY; (b) (6) DISL OSD POLICY; (b) (6) C CIV OSD POLICY; (b) (6) DISL DoD CIO; (b) (6) CAPT DoD CIO
Subject: Discussion Qs re monitoring & consent for DIB OPT-In Pilot Meeting, 9 Dec 2011, 0900-1200
Importance: High

Building on the initial list Charles provided, attached is DoD's suggested list of Qs regarding monitoring & consent practices -- to be released in advance to the DIB companies as preview of Friday's discussion, and also forming the basis for a survey/data-call that will follow immediately thereafter (informed by Friday's discussion).

PLEASE provide your edits, comments, or thumbs-ups as soon as practical today -- we'd like to send out to the DIBs ASAP. Sorry for the short-turn request.

THANKS! for your attention.

Cheers / (b) (6)

Attached: Survey-Discussion-Notice-Consent-Prx_draft4_07dec11.docx

(b) (6)
Associate General Counsel
DoD Office of the General Counsel
Direct: (b) (6)
(b) (6)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

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

From: (b) (6) Mr, DoD OGC
Sent: Monday, December 05, 2011 3:46 PM
To: (b) (6) Mr, DoD OGC; (b) (6) (b)(3)-P.L. 86-36 (b)(6)-P.L. 86-36
McDermott, Thomas M; Delaney, David; (b) (6), (b) (7)(C) (b) (6) Anderson,
Trisha (JMD); (b) (6) (b) (6) (b) (6)
Reheuser, Michael E SES OSD ODAM/DPCLO; (b) (6) DoD OGC; (b) (6)
DoD OGC
Subject: FW: DIB OPT-In Pilot Meeting, 9 Dec 2011, 0900-1200

FYI/SA - the invite w/agenda sent to the DIB companies.

(b) (6)
Associate General Counsel
DoD Office of the General Counsel
Direct: (b) (6)
(b) (6)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

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

From: (b) (6) DISL DoD CIO
Sent: Monday, December 05, 2011 2:45 PM
To *****
Cc: ** (b) (6) DISL OSD POLICY; (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36; (b) (6) DoD
OGC; (b) (6) DISL DoD CIO; (b) (6) CIV DoD CIO; (b) (6) CTR DoD CIO;
(b)(3)-P.L. 86-36 Conover, Brynn R'; (b)(3)-P.L. 86-36 L' (b) (6) (b) (6) CTR
DoD CIO; * Hale, Richard A SES DoD CIO; Carey, Robert J SES DoD CIO; (b) (6) CIV DoD CIO;
***** (b) (6) C CIV OSD POLICY
Subject: DIB OPT-In Pilot Meeting, 9 Dec 2011, 0900-1200

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Dear DIB Partners,

Please find attached the Agenda for the DIB Opt-In Pilot meeting, scheduled December 9, 2011, 0900-1200.

If you have not already done so, please RSVP to (b) (6) or (b) (6)
(b) (6) Please include the names of your participants in your RSVP. We

also encourage the participation of your General Counsel staff members to contribute to the legal discussion on the policies and practices regarding monitoring and consent. Due to space constraints, however, please limit your total attendees to no more than 3 participants.

LOCATION: The meeting will be held at the Institute for Defense Analyses, 4850 Center Drive, Alexandria, VA 22311 (Map/directions located on IDA website: <http://www.ida.org/directions.php>).

The security instructions for the DIB Opt-In Pilot meeting on December 9th are:

- The meeting will be conducted at the SECRET level. Please pass security clearance by December 7. FAX security clearance to IDA Security: (b) (6); Voice (b) (6). Include: Purpose of Visit: DIB Collaboration Meeting.
- Date of Visit: December 9, 2011 or pass security clearance via JPAS SMO Code: (b) (6). POCs are Mr. (b) (6)s and (b) (6)

We look forward to seeing you on December 9th.

Sincerely,
(b) (6)
Dir, DIB CS/IA

I'm assuming we (DHS) would require a PIA since this is related to the overall sensitive area of cybersecurity.

Although - there is a chance this could be limited to "fact of" malicious activity ("hey, we got hit with that phishing attack #27") versus actual traffic.

Then again, if they're sending over any data - including threat "indicators" which could include email addresses - then that could be PII-enough that we'd want to do a PIA.

(b) (5)

Alex Joel asked for a briefing. I haven't heard from (b) (6) - we just found out through Brown yesterday.

I'll let you know more as I learn it and will push back as though we are doing a public PIA.

Pete

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

voice: (b) (6) pager (b) (6) (b) (6) www.dhs.gov/privacy

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

From: Brown, Michael A. RADM
Sent: Thursday, March 24, 2011 3:03 PM
To: McNeely, James; Sand, Peter
Cc: Delaney, David; McDermott, Thomas M; (b) (6) Dean, Nicole M; (b) (6); (b)(3)-P.L. 86-3
Subject: FW: PA DIB Pilot Briefing Card 2011-03-17.doc

Team,

(b) (5)

v/r,
MAB

Mike Brown
RADM, USN
Director, Cybersecurity Coordination
National Protection & Programs Directorate Department of Homeland Security
(b) (6) (Fort Meade)
(b) (6) (Arlington)

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

From: Kudwa, Amy
Sent: Friday, March 18, 2011 1:35 PM
To: McConnell, Bruce; Brown, Michael A. RADM; Denning, John; (b) (6) (b) (6)
Subject: FW: PA DIB Pilot Briefing Card 2011-03-17.doc

With the caveat that I know everyone is stretched very thin right now, I received these DIB pilot TPs from DoD OPA this morning and they're seeking our input.

In speaking with (b) (6) they're not really getting incoming on this, but want to have something in the can for future use. She understands our operational posture at present, and so agreed that our getting back to her on Monday was fine. Can we internally aim for 10 a.m. Monday?

Thanks,
Amy

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

From: (b) (6) LtCol OSD PA (b) (6)
Sent: Friday, March 18, 2011 11:32 AM
To: 'Kudwa, Amy'
Subject: PA DIB Pilot Briefing Card 2011-03-17.doc

Amy,

As discussed yesterday, attached is DoD's DIB Opt In Pilot briefing card. The messages come from the coordinated communication plan that you all coordinated on, so there is nothing new.

V/r., (b) (6)

Andrew, Emily

From: Willis, Larry L.
Sent: Wednesday, January 11, 2012 11:41 AM
To: (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6); (b) (6); Andrew, Emily; Falkenstein, Cindy; (b) (6); Sanchious, Tony; Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up
Importance: High

(b)(3)-P.L. 86-36

Friday, 13 Jan 12 @ 9:30 a.m. is fine with me. I'll need to ensure Tony Sanchious (for Darryl Gingles (b) (6)) is ok with it.

What location?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Sent: Tuesday, January 10, 2012 2:58 PM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Subject: RE: JCPS IT Security Sync Up

Larry,

I understand that there is a meeting with AT&T on Friday and that some of you will probably attend that meeting. Since you are already up here, I suggest that we meet before the AT&T meeting. I am open that morning but have a 1100 and then the AT& meeting at 1300. How about 0930?

If Friday is not good for you, we will have to see about a time the following week. I have several meetings next week with the White House and I will have to work around that schedule.

BTW: I do not always look at my unclassified email. I spend 99% of my time on the classified system so emailing me on the classified side will reach me faster.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Monday, January 09, 2012 5:36 PM
To: (b) (6)

00848

Cc: Gingles, Darryl; (b) (6); (b) (6); (b) (6); (b) (6)
Falkenstein, Cindy; (b)(3)-P.L. 86-36; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

Dan,

Appreciate any assistance on getting this meeting set up.

Larry L. Willis
NCSO Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Willis, Larry L.
Sent: Monday, January 09, 2012 01:52 PM
To: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Cc: (b) (6); Gingles, Darryl; (b) (6); (b) (6); (b) (6); (b) (6)
Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Waiting for your reply.

Tks.

Larry L. Willis
NCSO Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: Willis, Larry L.
Sent: Thursday, January 05, 2012 11:15 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6); Gingles, Darryl; (b) (6); (b) (6); (b) (6); (b) (6)
Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up
Importance: High

Concur.

What are your available dates for the week of 9 Jan 12?

Tks.

Larry L. Willis
NCSO Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201

00849

Office: (b) (6)

Blackberry: (b) (6)

Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36

Sent: Wednesday, January 04, 2012 7:23 AM

To: Willis, Larry L.

Subject: RE: JCPS IT Security Sync Up

Larry,

My understanding is that there will be meetings with the ISPs this month so I would suggest that we meet before one of these meetings.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)

Sent: Wednesday, December 21, 2011 9:59 AM

To: (b)(3)-P.L. 86-36

Cc: (b) (6) Gingles, Darryl; (b) (6) Willis, Larry L.; (b) (6) (b) (6)

(b) (6) Falkenstein, Cindy

Subject: JCPS IT Security Sync Up

Importance: High

Good morning (b)(3)-P.L. 86-36 and hope that all is well.

The IT Security team here would like to sync up with you all as soon as possible in the new year. I know that next week is probably out of the question, so please provide a few dates during the first two weeks of Jan 12.

Tks.

Larry L. Willis

NCSD Security Manager, ISSM

Department of Homeland Security

Arlington, VA 22201

Office: (b) (6)

Blackberry: (b) (6)

Fax: (b) (6)

From: [Andrew, Emily](#)
To: [Falkenstein, Cindy](#)
Subject: FW: JCPS IT Security Sync Up
Date: Wednesday, January 11, 2012 4:34:28 PM

Cindy – my schedule is a bit crazy. Can you take this meeting for us and report back?

Thanks
Emily

From: Willis, Larry L.
Sent: Wednesday, January 11, 2012 1:23 PM
To: (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b)(6); (b)(6); (b)(6); Andrew, Emily; Falkenstein, Cindy; (b)(6); Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Friday @ 0930L is good. Please provide location; floor and room number.

Tks.

Larry L. Willis
NCS D Security Mgr/ISSM
B/B: (b)(6)
Sent via Blackberry

From: Sanchious, Tony
Sent: Wednesday, January 11, 2012 12:39 PM
To: Willis, Larry L.; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36>
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36 >; (b)(3)-P.L. 86-36; (b)(6); Gingles, Darryl; (b)(6); (b)(6); Andrew, Emily; Falkenstein, Cindy; (b)(6)
Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up

Larry,

That time is fine with me.

Tony

From: Willis, Larry L.
Sent: Wednesday, January 11, 2012 11:41 AM
To: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b)(6); (b)(6)

(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Sanchious, Tony; Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up
Importance: High

(b)(3)-P.L. 86-36

Friday, 13 Jan 12 @ 9:30 a.m. is fine with me. I'll need to ensure Tony Sanchious (for Darryl Gingles Office) is ok with it.

What location?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Tuesday, January 10, 2012 2:58 PM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Subject: RE: JCPS IT Security Sync Up

Larry,

I understand that there is a meeting with AT&T on Friday and that some of you will probably attend that meeting. Since you are already up here, I suggest that we meet before the AT&T meeting. I am open that morning but have a 1100 and then the AT& meeting at 1300. How about 0930?

If Friday is not good for you, we will have to see about a time the following week. I have several meetings next week with the White House and I will have to work around that schedule.

BTW: I do not always look at my unclassified email. I spend 99% of my time on the classified system so emailing me on the classified side will reach me faster.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Monday, January 09, 2012 5:36 PM
To: (b) (6)
Cc: Gingles, Darryl; (b) (6) (b) (6) (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; (b)(3)-P.L. 86-36 Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

Dan,

Appreciate any assistance on getting this meeting set up.

Larry L. Willis
NCSO Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Willis, Larry L.
Sent: Monday, January 09, 2012 01:52 PM
To: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Waiting for your reply.

Tks.

Larry L. Willis
NCSO Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: Willis, Larry L.
Sent: Thursday, January 05, 2012 11:15 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (CTR); (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up
Importance: High

Concur.

What are your available dates for the week of 9 Jan 12?

Tks.

Larry L. Willis
NCSO Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)

Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Wednesday, January 04, 2012 7:23 AM
To: Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Larry,

My understanding is that there will be meetings with the ISPs this month so I would suggest that we meet before one of these meetings.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Wednesday, December 21, 2011 9:59 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) Willis, Larry L.; (b) (6)
(b) (6) (b) (6) Falkenstein, Cindy
Subject: JCPS IT Security Sync Up
Importance: High

Good morning (b)(3)-P.L. 86-36 and hope that all is well.

The IT Security team here would like to sync up with you all as soon as possible in the new year. I know that next week is probably out of the question, so please provide a few dates during the first two weeks of Jan 12.

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: Willis, Larry L.
To: (b) (6)
Cc: (b) (6); (b) (6); Gingles, Darryl; (b) (6); (b) (6); Andrew, Emily; Falkenstein, Cindy; (b) (6); Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up
Date: Thursday, January 12, 2012 5:30:05 PM

(b)(3)-P.L. 86-36 Bob,

Please ensure we have a copy of the CONOPs for review in the morning as well as ALL related IT Sec docs.

Thanks.

Larry L. Willis
NCSD Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Willis, Larry L.
Sent: Thursday, January 12, 2012 11:10 AM
To: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6); (b) (6); Andrew, Emily; Falkenstein, Cindy; (b) (6); Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Ok.

We'll be there.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Sent: Thursday, January 12, 2012 10:21 AM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6); (b) (6); Andrew, Emily; Falkenstein, Cindy; (b) (6); Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony
Subject: RE: JCPS IT Security Sync Up

The meeting will be at NSA OPS 2A (b) (6)

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Wednesday, January 11, 2012 1:23 PM
To: (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6); (b) (6);
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Goode, Brendan; Shabat, Matthew; Campbell,
John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Friday @ 0930L is good. Please provide location; floor and room number.

Tks.

Larry L. Willis
NCSD Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Sanchious, Tony
Sent: Wednesday, January 11, 2012 12:39 PM
To: Willis, Larry L.; (b)(3)-P.L. 86-36 <(b)(3)-P.L. 86-36>
(b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl;
(b) (6); (b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6)
Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up

Larry,

That time is fine with me.

Tony

From: Willis, Larry L.
Sent: Wednesday, January 11, 2012 11:41 AM
To: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6); (b) (6);
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Sanchious, Tony; Goode, Brendan; Shabat,
Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up
Importance: High

(b)(3)-P.L. 86-36

Friday, 13 Jan 12 @ 9:30 a.m. is fine with me. I'll need to ensure Tony Sanchious (for
Darryl Gingles (b) (6) is ok with it.

What location?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Tuesday, January 10, 2012 2:58 PM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Subject: RE: JCPS IT Security Sync Up

Larry,

I understand that there is a meeting with AT&T on Friday and that some of you will probably attend that meeting. Since you are already up here, I suggest that we meet before the AT&T meeting. I am open that morning but have a 1100 and then the AT& meeting at 1300. How about 0930?

If Friday is not good for you, we will have to see about a time the following week. I have several meetings next week with the White House and I will have to work around that schedule.

BTW: I do not always look at my unclassified email. I spend 99% of my time on the classified system so emailing me on the classified side will reach me faster.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Monday, January 09, 2012 5:36 PM
To: (b) (6)
Cc: Gingles, Darryl; (b) (6) (b) (6) (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; (b)(3)-P.L. 86-36 Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

Dan,

Appreciate any assistance on getting this meeting set up.

Larry L. Willis
NCSD Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Willis, Larry L.
Sent: Monday, January 09, 2012 01:52 PM
To: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Waiting for your reply.

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: Willis, Larry L.
Sent: Thursday, January 05, 2012 11:15 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (b) (6) (b) (6)
(b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up
Importance: High

Concur.

What are your available dates for the week of 9 Jan 12?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Wednesday, January 04, 2012 7:23 AM
To: Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Larry,

My understanding is that there will be meetings with the ISPs this month so I would

suggest that we meet before one of these meetings.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Wednesday, December 21, 2011 9:59 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) Willis, Larry L.; (b) (6)
(b) (6) (b) (6) Falkenstein, Cindy
Subject: JCPS IT Security Sync Up
Importance: High

Good morning (b)(3)-P.L. 86-36 and hope that all is well.

The IT Security team here would like to sync up with you all as soon as possible in the new year. I know that next week is probably out of the question, so please provide a few dates during the first two weeks of Jan 12.

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: [Falkenstein, Cindy](#)
To: [Sand, Peter](#)
Cc: [Andrew, Emily](#)
Subject: FW: JCPS IT Security Sync Up
Date: Thursday, January 12, 2012 5:32:00 PM

Pete,

FYI: Just in case you have not seen the ConOps on the high side, Larry has asked that they provide at the morning meeting.

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: Willis, Larry L.
Sent: Thursday, January 12, 2012 5:30 PM
To: (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36; Gingles, Darryl; (b) (6) (b) (6)
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

Leslee/Bob,

Please ensure we have a copy of the CONOPs for review in the morning as well as ALL related IT Sec docs.

Thanks.

Larry L. Willis
NCSD Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Willis, Larry L.
Sent: Thursday, January 12, 2012 11:10 AM
To: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 Gingles, Darryl; (b) (6)
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Ok.

We'll be there.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Thursday, January 12, 2012 10:21 AM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 Gingles, Darryl; (b) (6) (b) (6)
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Goode, Brendan; Shabat, Matthew; Campbell,
John; Patterson, Larry S; Sanchious, Tony
Subject: RE: JCPS IT Security Sync Up

The meeting will be at NSA OPS 2A room (b) (6).

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Wednesday, January 11, 2012 1:23 PM
To: (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 Gingles, Darryl; (b) (6) (b) (6)
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Goode, Brendan; Shabat, Matthew; Campbell,
John; Patterson, Larry S; Sanchious, Tony; Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

(b)(3)-P.L. 86-36

Friday @ 0930L is good. Please provide location; floor and room number.

Tks.

Larry L. Willis
NCSD Security Mgr/ISSM
B/B: (b) (6)
Sent via Blackberry

From: Sanchious, Tony
Sent: Wednesday, January 11, 2012 12:39 PM
To: Willis, Larry L.; (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
(b) (6)
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36; (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36; Gingles, Darryl;
(b) (6) (b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6)
Goode, Brendan; Shabat, Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up

Larry,

That time is fine with me.

Tony

From: Willis, Larry L.
Sent: Wednesday, January 11, 2012 11:41 AM
To: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 Gingles, Darryl; (b) (6) (b) (6)
(b) (6) Andrew, Emily; Falkenstein, Cindy; (b) (6) Sanchious, Tony; Goode, Brendan; Shabat,
Matthew; Campbell, John; Patterson, Larry S
Subject: RE: JCPS IT Security Sync Up
Importance: High

(b)(3)-P.L. 86-36

Friday, 13 Jan 12 @ 9:30 a.m. is fine with me. I'll need to ensure Tony Sanchious (for Darryl Gingles (b) (6) is ok with it.

What location?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Tuesday, January 10, 2012 2:58 PM
To: Willis, Larry L.
Cc: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Subject: RE: JCPS IT Security Sync Up

Larry,

I understand that there is a meeting with AT&T on Friday and that some of you will probably attend that meeting. Since you are already up here, I suggest that we meet before the AT&T meeting. I am open that morning but have a 1100 and then the AT& meeting at 1300. How about 0930?

If Friday is not good for you, we will have to see about a time the following week. I have several meetings next week with the White House and I will have to work around that schedule.

BTW: I do not always look at my unclassified email. I spend 99% of my time on the classified system so emailing me on the classified side will reach me faster.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Monday, January 09, 2012 5:36 PM
To: (b) (6)
Cc: Gingles, Darryl; (b) (6) (b) (6) (b) (6) (b) (6)
 Falkenstein, Cindy; (b)(3)-P.L. 86-36 Willis, Larry L.
Subject: Re: JCPS IT Security Sync Up

Dan,

Appreciate any assistance on getting this meeting set up.

Larry L. Willis
 NCSD Security Mgr/ISSM
 B/B: (b) (6)
 Sent via Blackberry

From: Willis, Larry L.
Sent: Monday, January 09, 2012 01:52 PM
To: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (b) (6) (b) (6)
 (b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Leslee,

Waiting for your reply.

Tks.

Larry L. Willis
 NCSD Security Manager, ISSM
 Department of Homeland Security
 Arlington, VA 22201
 Office: (b) (6)
 Blackberry: (b) (6)
 Fax: (b) (6)

From: Willis, Larry L.
Sent: Thursday, January 05, 2012 11:15 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) (b) (6) (b) (6)
 (b) (6) Falkenstein, Cindy; Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up
Importance: High

Concur.

What are your available dates for the week of 9 Jan 12?

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

From: (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36
Sent: Wednesday, January 04, 2012 7:23 AM
To: Willis, Larry L.
Subject: RE: JCPS IT Security Sync Up

Larry,

My understanding is that there will be meetings with the ISPs this month so I would suggest that we meet before one of these meetings.

(b)(3)-P.L. 86-36

From: Willis, Larry L. (b) (6)
Sent: Wednesday, December 21, 2011 9:59 AM
To: (b)(3)-P.L. 86-36
Cc: (b) (6) Gingles, Darryl; (b) (6) Willis, Larry L.; (b) (6)
(b) (6) (b) (6) Falkenstein, Cindy
Subject: JCPS IT Security Sync Up
Importance: High

Good morning (b)(3)-P.L. 86-36 and hope that all is well.

The IT Security team here would like to sync up with you all as soon as possible in the new year. I know that next week is probably out of the question, so please provide a few dates during the first two weeks of Jan 12.

Tks.

Larry L. Willis
NCSD Security Manager, ISSM
Department of Homeland Security
Arlington, VA 22201
Office: (b) (6)
Blackberry: (b) (6)
Fax: (b) (6)

Andrew, Emily

From: Sand, Peter
 Sent: Friday, January 13, 2012 9:16 AM
 To: Andrew, Emily; Falkenstein, Cindy; (b) (6)
 Cc: PIA
 Subject: RE: PIA NPPD JCSP - DOD comments: PRA issue

Also - we are not collecting data from 10 or more individual using the same form... (I think that's the test), I'm not sure we're even asking any questions of anyone, we're just sending out data...

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).

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

From: Andrew, Emily
 Sent: Thursday, January 12, 2012 5:31 PM
 To: Sand, Peter; Falkenstein, Cindy; (b) (6)
 Cc: PIA
 Subject: Re: PIA NPPD JCSP - DOD comments

Pete,

I'll review when I get home but we said no to pra because this is business contact info and falls under the contacts pia. We were trying to keep those separate. Does that make sense?

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

From: Sand, Peter
 Sent: Thursday, January 12, 2012 05:26 PM
 To: Andrew, Emily; Falkenstein, Cindy; (b) (6) (b) (6)
 Cc: PIA
 Subject: PIA NPPD JCSP - DOD comments

Pete

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

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

From: (b) (6) CIV OSD POLICY (b) (6)
 Sent: Thursday, January 12, 2012 05:10 PM
 To: Sand, Peter; Goode, Brendan
 Cc: (b) (6) DISL DoD CIO (b) (6) >; Reheuser, Michael E SES OSD
 ODAM/DPCLO (b) (6); (b) (6) DISL OSD POLICY (b) (6)
 (b) (6), DoD OGC (b) (6) Schleien, Steven, SES, OSD-POLICY
 (b) (6); 'Shirley Steven SES DC3' (b) (6); (b) (6) CIV
 DoD CIO (b) (6); (b) (6) CTR DoD CIO (b) (6);
 (b) (6) CIV DoD CIO (b) (6) (b) (6) CTR DoD CIO
 (b) (6); France, Joyce SES DoD CIO (b) (6) (b) (6) CIV
 DoD CIO (b) (6)

Subject: FW: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Peter, Brendan,

Please find attached the consolidated comments from DoD. In addition to the attached, Mike Reheuser suggests the following change:

(b) (5)

Best,

(b) (6)
 Office of Cyber Policy
 Department of Defense
 (b) (6)

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

From: Sand, Peter (b) (6)
 Sent: Wednesday, January 11, 2012 8:29 PM
 To: Reheuser, Michael E SES OSD ODAM/DPCLO
 Subject: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Mike,

Attached please find the current version of the PIA for DHS's National Cyber Security Division

Joint Cybersecurity Services Pilot (JCSP) - DHS's extension of DOD's DIB Pilot.

We wanted to give you a chance to see it before it published. We're on a pretty tight deadline so if you do have comments, please send them back by 8 a.m. this Friday, January 13th.

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).

Andrew, Emily

From: Richards, Rebecca
Sent: Friday, January 13, 2012 10:21 AM
To: Sand, Peter; Andrew, Emily
Cc: Falkenstein, Cindy; PIA
Subject: RE: PIA NPPD JCSP - DOD comments
Attachments: DHS_PIA NPPD JCSP Draft 20120111 (2)_VM +DC3 edits-comments +MEC.doc

Attaching with MEC's small comments/changes.

I await the next version.
Becky

Becky Richards
DHS Privacy Office
(b) (6)

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

From: Sand, Peter
Sent: Friday, January 13, 2012 9:54 AM
To: Richards, Rebecca; Andrew, Emily
Cc: Falkenstein, Cindy; PIA
Subject: RE: PIA NPPD JCSP - DOD comments

Cindy,

DOD's line edits look fine to me. Their questions are more for US-CERT than us so I'm going to defer to you all on those.

(b) (5)

I'm not going to be able to make the 11:30 call and I'll be offline (on blackberry) from about 11:30 - 6:30, so I can work again after that if you need me for anything (and can work via blackberry in the mean time).

Otherwise, I say work directly with Becky since she also has MEC's comments.

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)

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

From: Richards, Rebecca

Sent: Friday, January 13, 2012 8:27 AM
To: Andrew, Emily; (b) (6)
Subject: Re: PIA NPPD JCSP - DOD comments

Her comments are easily handled whenever you want them -

(b) (5)

Everything else is nits. Tell me how to proceed. I am leaving at 1230 for NAC and back about 345.

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

From: Andrew, Emily
Sent: Friday, January 13, 2012 05:24 AM
To: Richards, Rebecca; (b) (6)
Subject: Re: PIA NPPD JCSP - DOD comments

Let's talk on how you want to handle. Those are just my edits, we have a call scheduled with US CERT to go over some of the questions and responses.

I'm gonna be at the NAC but will call when I can.

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

From: Richards, Rebecca
Sent: Thursday, January 12, 2012 10:09 PM
To: Andrew, Emily; (b) (6)
Subject: Fw: PIA NPPD JCSP - DOD comments

This is the version I should add MEC comments to? If so, will do and send to Pete, cindy, (b) (6) as soon as I get in.

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

From: Andrew, Emily
Sent: Thursday, January 12, 2012 09:26 PM
To: Andrew, Emily; (b) (6) Falkenstein, Cindy; Sand, Peter
Cc: Richards, Rebecca
Subject: RE: PIA NPPD JCSP - DOD comments

My computer is playing games again. Here's the version with my comments.

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

From: Andrew, Emily
Sent: Thursday, January 12, 2012 9:22 PM
To: (b) (6) Falkenstein, Cindy; Sand, Peter
Cc: Richards, Rebecca
Subject: FW: PIA NPPD JCSP - DOD comments

My comments are attached. I wanted to make sure you had them since I won't be in the office in the morning.

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

From: Sand, Peter
Sent: Thursday, January 12, 2012 5:27 PM
To: Andrew, Emily; Falkenstein, Cindy; (b) (6)
Cc: PIA

Subject: PIA NPPD JCSP - DOD comments

Pete

Peter E. Sand
DHS PRIV, (b) (6)
Sent via blackberry.

Please excuse the effects of big thumbs on little keys.

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

From: (b) (6) CIV OSD POLICY (b) (6)
Sent: Thursday, January 12, 2012 05:10 PM
To: Sand, Peter; Goode, Brendan
Cc: (b) (6) DISL DoD CIO (b) (6) Reheuser, Michael E SES OSD
ODAM/DPCLO (b) (6); (b) (6) DISL OSD POLICY (b) (6)
(b) (6) DoD OGC (b) (6) Schleien, Steven, SES, OSD-POLICY
(b) (6) 'Shirley Steven SES DC3' (b) (6) (b) (6) CIV
DoD CIO (b) (6) (b) (6) CTR DoD CIO (b) (6)
(b) (6) CIV DoD CIO (b) (6) (b) (6) CTR DoD CIO
(b) (6) France, Joyce SES DoD CIO (b) (6) (b) (6)
DoD CIO (b) (6)
Subject: FW: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Peter, Brendan,

Please find attached the consolidated comments from DoD. In addition to the attached, Mike Reheuser suggests the following change:

(b) (5)

Best,

(b) (6)
Office of Cyber Policy
Department of Defense
(b) (6)

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

From: Sand, Peter (b) (6)
Sent: Wednesday, January 11, 2012 8:29 PM
To: Reheuser, Michael E SES OSD ODA/DPCLO
Subject: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Mike,

Attached please find the current version of the PIA for DHS's National Cyber Security Division

Joint ⁰⁰⁸⁷⁰Cybersecurity Services Pilot (JCSP) - DHS's extension of DOD's DIB Pilot.

We wanted to give you a chance to see it before it published. We're on a pretty tight deadline so if you do have comments, please send them back by 8 a.m. this Friday, January 13th.

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)

Andrew, Emily

From: Andrew, Emily
Sent: Friday, January 13, 2012 10:39 AM
To: (b) (6)
Cc: Falkenstein, Cindy
Subject: FW: PIA NPPD JCSP - DOD comments
Attachments: DHS_PIA NPPD JCSP Draft 20120111 (2)_VM +DC3 edits-comments +MEC.doc

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

From: Richards, Rebecca
Sent: Friday, January 13, 2012 10:21 AM
To: Sand, Peter; Andrew, Emily
Cc: Falkenstein, Cindy; PIA
Subject: RE: PIA NPPD JCSP - DOD comments

Attaching with MEC's small comments/changes.

I await the next version.
Becky

Becky Richards
DHS Privacy Office
(b) (6)

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

From: Sand, Peter
Sent: Friday, January 13, 2012 9:54 AM
To: Richards, Rebecca; Andrew, Emily
Cc: Falkenstein, Cindy; PIA
Subject: RE: PIA NPPD JCSP - DOD comments

Cindy,

DOD's line edits look fine to me. Their questions are more for US-CERT than us so I'm going to defer to you all on those.

(b) (5)

I'm not going to be able to make the 11:30 call and I'll be offline (on blackberry) from about 11:30 - 6:30, so I can work again after that if you need me for anything (and can work via blackberry in the mean time).

Otherwise, I say work directly with Becky since she also has MEC's comments.

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).

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

From: Richards, Rebecca
Sent: Friday, January 13, 2012 8:27 AM
To: Andrew, Emily; (b) (6)
Subject: Re: PIA NPPD JCSP - DOD comments

Her comments are easily handled whenever you want them -

(b) (5)

Everything else is nits. Tell me how to proceed. I am leaving at 1230 for NAC and back about 345.

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

From: Andrew, Emily
Sent: Friday, January 13, 2012 05:24 AM
To: Richards, Rebecca; (b) (6)
Subject: Re: PIA NPPD JCSP - DOD comments

Let's talk on how you want to handle. Those are just my edits, we have a call scheduled with US CERT to go over some of the questions and responses.

I'm gonna be at the NAC but will call when I can.

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

From: Richards, Rebecca
Sent: Thursday, January 12, 2012 10:09 PM
To: Andrew, Emily; (b) (6)
Subject: Fw: PIA NPPD JCSP - DOD comments

This is the version I should add MEC comments to? If so, will do and send to Pete, cindy, (b) (6) as soon as I get in.

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

From: Andrew, Emily
Sent: Thursday, January 12, 2012 09:26 PM
To: Andrew, Emily; (b) (6) Falkenstein, Cindy; Sand, Peter
Cc: Richards, Rebecca
Subject: RE: PIA NPPD JCSP - DOD comments

My computer is playing games again. Here's the version with my comments.

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

From: Andrew, Emily
Sent: Thursday, January 12, 2012 9:22 PM
To: (b) (6) Falkenstein, Cindy; Sand, Peter
Cc: Richards, Rebecca
Subject: FW: PIA NPPD JCSP - DOD comments

My comments are attached. I wanted to make sure you had them since I won't be in the office in the morning.

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

From: Sand, Peter
Sent: Thursday, January 12, 2012 5:27 PM
To: Andrew, Emily; Falkenstein, Cindy; (b) (6)
Cc: PIA
Subject: PIA NPPD JCSP - DOD comments

Pete

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

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

From: (b) (6) CIV OSD POLICY (b) (6)
Sent: Thursday, January 12, 2012 05:10 PM
To: Sand, Peter; Goode, Brendan
Cc: (b) (6) DISL DoD CIO (b) (6) Reheuser, Michael E SES OSD
ODAM/DPCLO (b) (6) (b) (6) DISL OSD POLICY (b) (6)
(b) (6), DoD OGC (b) (6) Schleien, Steven, SES, OSD-POLICY
(b) (6) 'Shirley Steven SES DC3' (b) (6) (b) (6) CIV
DoD CIO (b) (6) (b) (6) CTR DoD CIO (b) (6)
(b) (6) CIV DoD CIO (b) (6) (b) (6) CTR DoD CIO
(b) (6) France, Joyce SES DoD CIO (b) (6) (b) (6) CIV
DoD CIO (b) (6)
Subject: FW: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Peter, Brendan,

Please find attached the consolidated comments from DoD. In addition to the attached, Mike Reheuser suggests the following change:

(b) (5)

Best,

(b) (6) y
Office of Cyber Policy
Department of Defense
(b) (6)

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

From: Sand, Peter (b) (6)
Sent: Wednesday, January 11, 2012 8:29 PM
To: Reheuser, Michael E SES OSD ODA/DPCLO

Subject: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Mike,

Attached please find the current version of the PIA for DHS's National Cyber Security Division

Joint Cybersecurity Services Pilot (JCSP) - DHS's extension of DOD's DIB Pilot.

We wanted to give you a chance to see it before it published. We're on a pretty tight deadline so if you do have comments, please send them back by 8 a.m. this Friday, January 13th.

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)

Andrew, Emily

From: Sand, Peter
Sent: Saturday, January 14, 2012 7:53 AM
To: (b) (6) CIV OSD POLICY; Goode, Brendan
Cc: (b) (6) DISL DoD CIO; Reheuser, Michael E SES OSD ODAM/DPCLO; (b) (6) DISL OSD POLICY; (b) (6) DoD OGC; Schleien, Steven, SES, OSD-POLICY; 'Shirley Steven SES DC3'; (b) (6) CIV DoD CIO; (b) (6) CTR DoD CIO; (b) (6) CIV DoD CIO; (b) (6) CTR DoD CIO; France, Joyce SES DoD CIO; (b) (6) CIV DoD CIO; Callahan, Mary Ellen; Andrew, Emily; Rebecca J. Richards (b) (6) Falkenstein, Cindy
Subject: RE: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP
Attachments: DHS PIA NPPD JCSP Draft 20120111 DOD cmts resp.doc; privacy_nppd_jcsp_pia.pdf

(b) (6)

Thank you for reviewing the draft PIA. Attached is a draft back with responses to your comments as well as an advance copy of the final PIA. I will send you the URL to the PIA when it publishes - should be on this page near the top:
https://www.dhs.gov/files/publications/gc_1284567214689.shtm

Thanks again,

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).

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

From: (b) (6) CIV OSD POLICY (b) (6)
Sent: Thursday, January 12, 2012 5:10 PM
To: Sand, Peter; Goode, Brendan
Cc: (b) (6) DISL DoD CIO; Reheuser, Michael E SES OSD ODAM/DPCLO; (b) (6) DISL OSD POLICY; (b) (6) Mr, DoD OGC; Schleien, Steven, SES, OSD-POLICY; 'Shirley Steven SES DC3'; (b) (6) CIV DoD CIO; (b) (6) CTR DoD CIO; (b) (6) CIV DoD CIO; (b) (6) CTR DoD CIO; France, Joyce SES DoD CIO; (b) (6) CIV DoD CIO
Subject: FW: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Peter, Brendan,

Please find attached the consolidated comments from DoD. In addition to the attached, Mike Reheuser suggests the following change:

(b) (5)

(b) (5)

Best,

(b) (6)

Office of Cyber Policy
Department of Defense

(b) (6)

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

From: Sand, Peter (b) (6)
Sent: Wednesday, January 11, 2012 8:29 PM
To: Reheuser, Michael E SES OSD ODAM/DPCLD
Subject: [FYI/Review: Friday 8 a.m., 01/13/2012] PIA NPPD JCSP

Mike,

Attached please find the current version of the PIA for DHS's National Cyber Security Division

Joint Cybersecurity Services Pilot (JCSP) - DHS's extension of DOD's DIB Pilot.

We wanted to give you a chance to see it before it published. We're on a pretty tight deadline so if you do have comments, please send them back by 8 a.m. this Friday, January 13th.

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: [Callahan, Mary Ellen](#); (b) (6); [Sand, Peter](#); [Falkenstein, Cindy](#)
Subject: Fw: DIB Activities, Communication Plan and Other Roducts
Date: Tuesday, May 15, 2012 6:26:46 PM
Attachments: [20120510 FINAL DIB ECSS Comms Plan.pdf](#)
[20120411 DIB Activities Communication Matrix-FINAL.pdf](#)
[Fact Sheet - DIB Activities-FINAL.pdf](#)

FYI

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

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

From: Davis, Robert M
Sent: Tuesday, May 15, 2012 02:20 PM
To: Gillis, Ryan M; Andrew, Emily
Subject: Fw: DIB Activities, Communication Plan and Other Roducts

FYI

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

From: (b) (6) OSD PA (b) (6)
Sent: Monday, May 14, 2012 03:47 PM
To: Jensen, Robert; Boogaard, Peter; (b) (6) Davis,
Robert M; (b) (6) (b) (6)
Subject: DIB Activities, Communication Plan and Other Roducts

ALCON: FYSA, final products are attached.

Other Products:

Press Release: <http://www.defense.gov/releases/release.aspx?releaseid=15266>

AFPS: <http://www.defense.gov/news/newsarticle.aspx?id=116306>

The Pentagon Channel: Go to "www.pentagonchannel.mil" and research "defense industrial base

Initial Articles (Embargoed Interviews):

Pentagon to expand cybersecurity program for defense contractors

By Ellen Nakashima

http://www.washingtonpost.com/world/national-security/pentagon-to-expand-cybersecurity-program-for-defense-contractors/2012/05/11/gIOALhjbHU_story.html

The Pentagon is expanding and making permanent a trial program that teams the government with Internet carriers to protect defense firms' computer networks against massive data theft by foreign adversaries.

Pentagon Says Cyber-Threat Sharing May Reach 1,000 Contractors
<http://www.bgov.com/news_item/jekRc6r9gc8dsAHQwBid4Q>

(Bloomberg) -- The Pentagon predicts as many as 1,000 defense contractors may join a voluntary effort to share classified information on cyber threats under an expansion of a first-ever initiative to protect computer networks.

After a four-year pilot program involving 36 contractors and three of the biggest U.S. Internet providers, the Obama administration approved a rule letting the Pentagon enlist all contractors and Internet providers with security clearances in the information exchange, according to Eric Rosenbach, deputy assistant secretary of defense for cyber policy.

"This is an important milestone in voluntary information-sharing between government and industry," Rosenbach said in an interview yesterday at the Pentagon. Richard Hale, the Pentagon's deputy chief information officer for cybersecurity, said that 1,000 companies may participate.

If the Pentagon's effort proves successful in safeguarding defense contractors from cyber attacks, the administration may enlarge the program to companies in 15 other critical infrastructure categories through the Department of Homeland Security, Rosenbach said.

Cyber threats facing the U.S. defense industry and its "unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests," according to the federal rule authorizing the expanded Department of Defense program.

Secure Portal

Using a secure portal called DIBnet, the Pentagon will provide both classified and unclassified information on cybersecurity threats and defenses against them to companies that have security clearances and agree to participate, according to Rosenbach and Hale said.

"You are using special intelligence information derived somewhere else in the world to put into" cybersecurity, Rosenbach said in the interview. "So it is more active than simply waiting for an attack to come."

Internet providers such as Verizon Communications Inc. <<http://www.bgov.com/companies/100185>> and defense contractors including Lockheed Martin Corp. <<http://www.bgov.com/companies/156923>> have said they participated in the pilot program and intended to continue in an expanded effort.

"We might share with the companies what kind of cyber attack trends we are seeing inside DoD -- if a particular kind of phishing attack, for instance, has become more prevalent," Hale said.

Participants may also elect to join a "enhanced effort" under which the Defense Department will provide fixes for each type of threat to Internet providers and other eligible companies that in turn will screen the network traffic flowing to contractors, Rosenbach said.

Cybersecurity Services

Lockheed, based in Bethesda, Maryland, and New York-based Verizon have said they would take the Pentagon-provided information and offer a package of cybersecurity services for a fee to other contractors. The companies have said they are working to determine how much customers would have to pay for such services that draw on the U.S. intelligence.

Booz Allen Hamilton Holding Corp. and SAIC Inc. <<http://www.bgov.com/companies/10002321>> , both based in McLean, Virginia, and Computer Sciences Corp. <<http://www.bgov.com/companies/100375>> , based in Falls Church, Virginia, participated in developing and running the cyber information-sharing program, according to Jason Wilson, an analyst with Bloomberg Government. In addition to Verizon, Internet-providers AT&T Inc. and CenturyLink Inc., joined the pilot program.

Very Respectfully,

(b) (6)

(b) (6)

(b) (6) U.S. Air Force

Public Affairs Officer for:

Office of the Secretary of Defense (OSD); Assistant Secretary of Defense for Global Strategic Affairs and
Department of Defense Chief Information Officer 1400 Defense Pentagon (b) (6) Washington, DC

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DIB Cyber Pilot

Location: Institute For Defense Analysis
Alexandria, VA
December 9, 2011 (9:00 am-12:00 pm ET)

AGENDA

9:00 – 9:15	Welcome and Introductions	DoD
9:15 – 9:35	Status Update and Path Forward on the DIB Pilot Evaluation and Extension	DoD, DHS
9:35 – 11:55	Legal Discussion: Policies and Practices Regarding Monitoring and Consent <ul style="list-style-type: none">• Update/Lessons Learned by DIB Partners Regarding Assessment and Implementation of Consent Mechanisms (DIB Companies)• Feedback and Discussion of Pilot Legal Construct for Addressing Consent and Monitoring – Recommendations for the Way Ahead (Open Discussion)	DoD, DHS, DoJ, DIB
11:55 – 12:00	Closing Comments and Next Steps	DoD, DHS

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DISCUSSION TOPICS REGARDING MONITORING & CONSENT PRACTICES

FOR USG-DIB MEETING ON DECEMBER 09, 2011

NOTE: PARTICIPATION IS 100% VOLUNTARY. ALL DISCUSSIONS WILL BE NON-ATTRIBUTIONAL AND ANY MATERIALS SUBMITTED WILL BE ANONYMIZED.

1. Was the pre-pilot guidance (*e.g.*, the 8 key elements for notice & consent banners) provided by the USG valuable in identifying or addressing these issues?
 - a. Were there any elements of the guidance that were not clear, not applicable, or otherwise not helpful?
 - b. Is there any additional information, or other forms of assistance, that might be more helpful?
2. Has your company elected to revise or update its logon banners or other means by which it obtains user consent? (Or are you considering doing so now, or in the near future?)
 - a. If so, were these updates facilitated by the guidance or discussion of these issues in connection with the pilot? What types of considerations drove these changes?
 - b. What are the primary challenges, and the typical time frames required, in making changes to your company's logon banner or other mechanisms used to secure consent?
3. As an update to the previous survey of notice & consent practices initiated in December 2010:
 - a. What are the primary mechanism(s) your company uses to achieve user notice and consent (*e.g.*, logon banners, user agreements, workplace policies, employee training).
 - b. What is the operative language your company uses to obtain user consent for monitoring and disclosure of information (*e.g.*, copies of logon banners or user agreements, excerpts from company policies or employee training, description of other notice procedures).
4. Has your company experienced any unanticipated issues or significant challenges regarding implementation of its notice & consent mechanisms? If so, please describe them.
5. Some companies have indicated that they also rely significantly on legal theories other than notice & consent (*e.g.*, "rights and property") for some elements of their information security practices. What are the other legal theories or mechanisms (*i.e.*, other than notice & consent) that may apply to the types of monitoring or information sharing activities under with the DIB pilot? *Note: this question is not intended to elicit any specific, attorney-client privileged information -- only to identify applicable legal theories.*
6. The DIB pilot activity utilized a certification approach regarding each company's individual determination of the legality of its policies and practices, including user notice & consent –
 - a. Would this approach be effective in a permanent DIB program with expanded participation?
 - b. Are there other approaches to addressing these legal issues that should be considered?
 - c. Do you have any other recommendations or suggestions for addressing these issues in any future implementation of the DIB pilot or related information sharing activities?

Survey Questions: Monitoring and Consent Practices

NOTE: RESPONSE TO THE SURVEY IS 100% VOLUNTARY. THE DIB CS/IA PROGRAM OFFICE WILL ANONYMIZE ALL RESPONSES.

1. Was the pre-pilot guidance (*e.g.*, the 8 key elements for notice & consent banners) provided by the USG valuable in identifying or addressing these issues?
 - a. Were there any elements of the guidance that were not clear, not applicable, or otherwise not helpful?
 - b. Is there any additional information, or other forms of assistance, that might be more helpful?
2. Has your company elected to revise or update its logon banners or other means by which it obtains user consent? (Or are you considering doing so now, or in the near future?)
 - a. If so, were these updates facilitated by the guidance or discussion of these issues in connection with the pilot? What types of considerations drove these changes?
 - b. What are the primary challenges, and the typical time frames required, in making changes to your company's logon banner or other mechanisms used to secure consent?
3. As an update to the previous survey of notice and consent practices initiated in December 2010:
 - a. What are the primary mechanism(s) your company uses to achieve user notice and consent (*e.g.*, log-on banners, user agreements, workplace policies, employee training).
 - b. What is the operative language your company uses to obtain user consent for monitoring and disclosure of information (*e.g.*, copies of logon banners or user agreements, excerpts from company policies or employee training, description of other notice procedures).
4. Has your company experienced any unanticipated issues or significant challenges regarding implementation of its notice & consent mechanisms? If so, please describe them.
5. Some companies have indicated that they also rely significantly on legal theories other than notice & consent (*e.g.*, "rights and property") for some elements of their information security practices. What are the other legal theories or mechanisms (*i.e.*, other than notice and consent) that may apply to the types of monitoring or information sharing activities under with the DIB pilot? *Note: this question is not intended to elicit any specific, attorney-client privileged information -- only to identify applicable legal theories.*
6. The DIB pilot activity utilized a certification approach regarding each company's individual determination of the legality of its policies and practices, including user notice & consent –
 - a. Would this approach be effective in a permanent DIB program with expanded participation?
 - b. Are there other approaches to addressing these legal issues that should be considered?
 - c. Do you have any other recommendations or suggestions for addressing these issues in any future implementation of the DIB pilot or related information sharing activities?

DoD Office of General Counsel

Legal Discussion: Policies and Practices Regarding Monitoring and Consent



DIB Cybersecurity Pilot Meetings
December 09, 2011

(b) (6)

Associate General Counsel
DoD Office of the General Counsel

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Disclaimer

- This briefing is being provided for informational and discussion purposes only and does not constitute legal advice, nor create any attorney-client relationship. The Department of Defense Office of General Counsel is not acting as your attorney. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this briefing. We likewise do not warrant the legal effect of these materials.
- The law changes very rapidly and, accordingly, we do not guarantee the accuracy or currency of this information is accurate and up to date. The law differs from jurisdiction to jurisdiction, and is subject to interpretation of courts located in each state or county. Legal advice must be tailored to the specific circumstances of each case and the tools and information provided to you may not be an appropriate fit in your case.
- The opinions expressed in the presentation of these materials are those of the individual contributors to or presenters of these materials and do not necessarily represent, and should not be attributed to, the Department of Defense or the United States Government.


UNCLASSIFIED//FOR OFFICIAL USE ONLY



Agenda

9:00 – 9:15	Welcome and Introductions	DoD
9:15 – 9:35	Status Update and Path Forward on the DIB Pilot Evaluation and Extension	DoD, DHS
9:35 – 11:55	Legal Discussion: Policies and Practices Regarding Monitoring and Consent <ul style="list-style-type: none"> • Update/Lessons Learned by DIB Partners Regarding Assessment and Implementation of Consent Mechanisms (DIB Companies) • Feedback and Discussion of Pilot Legal Construct for Addressing Consent and Monitoring -- Recommendations for the Way Ahead (Open Discussion) 	DoD, DHS, DoJ, DIB
11:55 – 12:00	Closing Comments and Next Steps	DoD, DHS

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



More Specifically

9:35 – 11:55	Legal Discussion: Policies and Practices Regarding Monitoring and Consent <ul style="list-style-type: none"> • Update/Lessons Learned by DIB Partners Regarding Assessment and Implementation of Consent Mechanisms • Feedback and Discussion of Pilot Legal Construct for Addressing Consent and Monitoring -- Recommendations for the Way Ahead 	DoD, DHS, DoJ, DIB DIB Companies Open Discussion
--------------	---	--

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



Please Keep in Mind...

1. The “Discussion Topics Regarding Monitoring & Consent Practices” is a SUGGESTED LIST of topics – to encourage and offer structure to an open discussion of complex issues . . . not intended to limit
2. Participation in the discussion or survey activities is absolutely 100% VOLUNTARY.
3. All of the discussions will be NON-ATTRIBUTIONAL.
4. Any written responses, or other documentary materials (e.g., samples of updated banner language), will be ANONYMIZED – with several options for doing so

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Excerpt from the FA Amendment

Under SECTION X: GENERAL PROVISIONS, *Add the following:*

- “L. The Parties will conduct their respective activities under this FA, including all amendments and attachments, in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. By signing FA Amendment #–
- “1. The Government is confirming that it has performed a review of its policies and practices that support Government activities under this FA, and has determined that such policies, practices, and activities comply with applicable legal requirements; and
 - “2. The Company is confirming that it has performed a review of its policies and practices that support Company activities under this FA, and has determined that such policies, practices, and activities comply with applicable legal requirements, and include measures that the Company has determined are legally sufficient to ensure authorized user consent to the interception, monitoring, access, use, and disclosure of electronic communications or data residing on or transiting Company systems, including the disclosure of related information to the Government as provided in this FA.”

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Discussion Topics

1. Was the pre-pilot guidance (e.g., the 8 key elements for notice & consent banners) provided by the USG valuable in identifying or addressing these issues?
 - a. Were there any elements of the guidance that were not clear, not applicable, or otherwise not helpful?
 - b. Is there any additional information, or other forms of assistance, that might be more helpful?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

7



Discussion Topics

2. Has your company elected to revise or update its logon banners or other means by which it obtains user consent? (Or are you considering doing so now, or in the near future?)
 - a. If so, were these updates facilitated by the guidance or discussion of these issues in connection with the pilot? What types of considerations drove these changes?
 - b. What are the primary challenges, and the typical time frames required, in making changes to your company's logon banner or other mechanisms used to secure consent?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

8



Discussion Topics

3. As an update to the previous survey of notice & consent practices initiated in December 2010:
 - a. What are the primary mechanism(s) your company uses to achieve user notice and consent (e.g., log-on banners, user agreements, workplace policies, employee training).
 - b. What is the operative language your company uses to obtain user consent for monitoring and disclosure of information (e.g., copies of logon banners or user agreements, excerpts from company policies or employee training, description of other notice procedures).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

9



Discussion Topics

4. Has your company experienced any unanticipated issues or significant challenges regarding implementation of its notice & consent mechanisms? If so, please describe them.
5. Some companies have indicated that they also rely significantly on legal theories other than notice & consent (e.g., "rights and property") for some elements of their information security practices. What are the other legal theories or mechanisms (i.e., other than notice & consent) that may apply to the types of monitoring or information sharing activities under with the DIB pilot? *Note: this question is not intended to elicit any specific, attorney-client privileged information -- only to identify applicable legal theories.*

UNCLASSIFIED//FOR OFFICIAL USE ONLY

10



Discussion Topics

6. The DIB pilot activity utilized a certification approach regarding each company's individual determination of the legality of its policies and practices, including user notice & consent –
- a. Would this approach be effective in a permanent DIB program with expanded participation?
 - b. Are there other approaches to addressing these legal issues that should be considered?
 - c. Do you have any other recommendations or suggestions for addressing these issues in any future implementation of the DIB pilot or related information sharing activities?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

11




Discussion Topics

**Did we miss
anything?**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

12




Questions?

(b) (6)

Associate General Counsel
Department of Defense
Office of the General Counsel


Direct: **(b) (6)**

(b) (6)



UNCLASSIFIED//FOR OFFICIAL USE ONLY

13



BACKUP SLIDES

UNCLASSIFIED//FOR OFFICIAL USE ONLY

14

DoD Office of General Counsel

Discussion Points: Key Elements for Notice and Consent Banners



Defense Industrial Base Cybersecurity
Exploratory Initiative Meetings
December 2-3 2010

(b) (6)

Associate General Counsel
Department of Defense
Office of the General Counsel

UNCLASSIFIED//FOR OFFICIAL USE ONLY

15



Overview

8 Key Elements for Notice and Consent Banners

1. It expressly covers *monitoring* of data and communications *in transit* rather than just accessing data *at rest*.
2. It provides that information transiting or stored on the system may be *disclosed* for any purpose, including to the Government.
3. It states that monitoring will be *for any purpose*.
4. It states that monitoring may be done by the Company/Agency or *any person or entity authorized by Company/Agency*.
5. It explains to users that they have "*no [reasonable] expectation of privacy*" regarding communications or data transiting or stored on the system.
6. It clarifies that this consent covers *personal use* of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.
7. It is *definitive* about the fact of monitoring, rather than conditional or speculative.
8. It expressly *obtains consent* from the user and does not merely provide notification.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

16



-
1. It expressly covers **monitoring** of data and communications **in transit** rather than just accessing data **at rest**.

Notes:

- Use the terms “monitoring” and/or “intercept.”
- This requirement is driven by the Wiretap Act and Stored Communications Act.

Examples:

- “You consent to the unrestricted monitoring, interception...of all communications and data transiting or stored on this system....”
- “You consent, without restriction, to all communications and data transiting or stored on this system being monitored, intercepted...”

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

17



-
2. It provides that information transiting or stored on the system may be **disclosed** for any purpose, **including to the Government**.

Notes:

- Both access and disclosure must be addressed in the banner.
- Unauthorized disclosure is a separate crime from unauthorized access under statute.

Example:

- “You consent, without restriction, to all communications and data transiting or stored on this system being monitored...or disclosed to any entity, including to the Government...”

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

18



3. It states that monitoring will be *for any purpose*.

Examples:

- "...at any time and for any purpose..."
- "...at any time and for any purpose, including for cybersecurity purposes..."
- "...for any lawful purpose..."

UNCLASSIFIED//FOR OFFICIAL USE ONLY

19



4. It states that monitoring may be done by the Company/Agency or *any person or entity authorized by Company/Agency*.

Examples:

- "...monitoring by or disclosure to any entity authorized by [Company]..."
- "...monitoring by or disclosure to any entity... at the sole discretion of [Company]."

UNCLASSIFIED//FOR OFFICIAL USE ONLY

20



5. It explains to users that they have “no [reasonable] expectation of privacy” regarding communications or data transiting or stored on the system.

Notes:

- This language tracks the case law analyses at both federal level and many State laws
- Legally significant “buzz phrase”.

Example:

- “You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system...”

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

21



6. It clarifies that this consent covers *personal use* of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.

Notes:

- People may develop an expectation of privacy in their personal communications if they can access them from work. This needs to be explicitly addressed.

Example:

- “...including work-related use and personal use without exception...”

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

22



7. It is **definitive** about the fact of monitoring, rather than conditional or speculative.

Notes:

- If the language is too conditional with regard to monitoring, users begin to develop an expectation of privacy over time.
- In addition to definitive banner language, there should be no other representations that actual monitoring doesn't happen, or happens only seldom, in practice.

Example:

- "...will be monitored..." AVOID "may be" OR "reserves the right to"

UNCLASSIFIED//FOR OFFICIAL USE ONLY

23



8. It expressly **obtains consent** from the user and does not merely provide notification.

Notes:

- Click-through banners are best because they force the user to interact with the language.
- Supporting processes should also preserve/provide evidence of the user's agreement to the terms.

Examples:

- "By using this system, you are acknowledging and consenting to..."
- "By clicking [ACCEPT] below... you consent to..."

UNCLASSIFIED//FOR OFFICIAL USE ONLY

24



And the [almost] unspoken factor...

The rest of the banner ...

(or associated policies, elements of user
agreement, user training, etc.) ...

must not be inconsistent with, or
otherwise undercut, these elements.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

25

DEPARTMENT OF DEFENSE**(b) (2)****Office of the Secretary****DOD-2009-OS-0183/RIN 0790-AI60****32 CFR PART 236****Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities****AGENCY:** Office of the DoD Chief Information Officer, DoD**ACTION:** Interim final rule

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

DATES: This rule is effective upon publication in the Federal Register. Comments must be received by [insert 30 days from date of publication in the Federal Register].

ADDRESSES: You may submit comments, identified by docket number and/or RIN number and title, by any of the following methods:

- **Federal Rulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **Mail:** Federal Docket Management System Office, 4800 Mark Center Drive, 2nd Floor East Tower, Suite 02G09, Alexandria, VA 22350-3100.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this Federal Register document. The general policy

for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: DIB Cyber Security and Information Assurance Program Office, (703) 604-3167.

SUPPLEMENTARY INFORMATION:

Background.

Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. DoD's voluntary DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

DIB CS/IA activities, including the collection, management and sharing of information for cyber security purposes, support and implement the following national and DoD-specific guidance and authority: information assurance (IA) requirements to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities (see 10 U.S.C. § 2224; and the Federal Information Security Management Act (FISMA), codified at 44 U.S.C. §§ 3541 et seq.); critical infrastructure protection responsibilities, in which DoD is the sector specific agency for the DIB sector, (see Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection,"); and other

federal cyber security initiatives and activities (see National Security Presidential Directive (NSPD) 54/HSPD 23 (which formalizes the Comprehensive National Cyber Security Initiative)). The DoD established the voluntary DIB CS/IA program to enhance and supplement DIB participant's capabilities to safeguard DoD unclassified information that resides on, or transits, DIB unclassified information systems. At the core of the program is a bilateral cyber security information sharing activity, in which DoD provides cyber threat information and information assurance (IA) best practices to DIB companies to enhance and supplement DIB companies' capabilities to safeguard DoD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents to the DoD-DIB Collaborative Information Sharing Environment (DCISE), located at DC3. The DoD analyzes the information reported by the DIB company regarding any such cyber incident, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures. In addition to this initial reporting and analysis, the DoD and DIB company may pursue, on a voluntary basis, follow-on, more detailed, digital forensics analysis or damage assessments, including sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information. The information sharing arrangements between the DoD and each participating DIB company are memorialized in a standardized bilateral Framework Agreement (FA). As part of DoD's instantiation of the voluntary DIB CS/IA program, DoD developed new policies and procedures, developed a dedicated threat sharing and collaboration system, and validated on-line application procedures in order to support participation by a large number of companies. The on-line application procedures provide the administrative and security requirements for DIB participants, including the standardized bilateral FA that implements the requirements of the DIB CS/IA program. The FA will typically be executed by a senior DoD

official, such as the DoD Chief Information Officer (CIO), and by a DIB company corporate senior official (e.g., Company CIO or equivalent).

This interim-final rule establishes a new part 236 in title 32 of the Code of Federal Regulations, with the following new sections: Section 236.2 establishes the definitions of terms used in the new part, leveraging established definitions to the maximum extent possible (e.g., those provided in the Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary"); Section 236.4 sets forth the basic requirements and procedures of the voluntary program, including information collection requirements; Section 236.5 characterizes cyber security information sharing and collection procedures; Section 236.6 establishes the general provisions of the voluntary DIB CS/IA program; and Section 236.7 sets forth the eligibility requirements to participate in the voluntary program.

Nothing in this rule or program is intended to be inconsistent with any other related or similar federal agency or private sector activity or requirement. For example, nothing in this rule or program abrogates the Government's or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation.

Similarly, this rule and program are intended to be consistent and coordinated with, and updated as necessary to ensure consistency with and support for, other federal activities related to the handling and safeguarding of controlled unclassified information, such as those that are being led by the National Archives and Records Administration pursuant to Executive Order 13556 "Controlled Unclassified Information" (November 4, 2010) (see <http://www.archives.gov/cui/>).

Executive Orders 12866, “Regulatory Planning and Review” and 13563, “Improving Regulation and Regulatory Review”

It has been certified that 32 CFR part 236 does not:

- (a) Have an annual effect on the economy of \$100 million or more, or adversely affect in a material way, the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;
- (b) Create a serious inconsistency, or otherwise interfere with, an action taken or planned by another Agency;
- (c) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or
- (d) Raise novel legal or policy issues arising out of legal mandates, the President’s priorities, or the principles as set forth in these Executive Orders.

Public Law 104-121, “Congressional Review Act” (5 U.S.C. 801)

It has been determined that 32 CFR part 236 is not a “major” rule under 5 U.S.C. 801, enacted by Public Law 104-121, because it will not result in an annual effect on the economy of \$100 million or more; a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

Sec. 202, Public Law 104-4, “Unfunded Mandates Reform Act”

It has been certified that 32 CFR part 236 does not contain a Federal mandate that may result in expenditure by State, local and tribal governments, in aggregate, or by the private sector, of \$100 million or more in any one year.

Public Law 96-354, “Regulatory Flexibility Act” (5 U.S.C. 601)

It has been certified that 32 CFR part 236 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. DIB participation in the DIB CS/IA Program is voluntary.

Public Law 96-511, “Paperwork Reduction Act” (44 U.S.C. Chapter 35)

Sections 236.4 and 236.5 and 236.7 of this interim final rule contain information collection requirements. DoD has submitted the following proposal to Office of Management and Budget (OMB) under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the proposed information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

(a) Title: *Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Points of Contact Information*

Type of Request: New.

Projected Responses Per Respondent: One response is required initially and thereafter only on an “as needed/required” basis, as changes to the points of contact occur.

Annual Responses: 275, which includes the additional responses required on an “as needed/required” basis.

Average Burden Per Response: 20 minutes.

Annual Burden Hours: Total annual burden for respondents 92 hours.

Total Annualized Cost to Respondents: One-time cost of ~\$12 per respondent. Total cumulative annual cost for 250 respondents (275 responses) is \$3,337.

Needs and Uses: The DIB CS/IA program collects Point of Contact (POC) information from DIB participants. POC information is needed to facilitate communication between DoD and DIB participants, as well as prospective participants. The POC information includes the names, security clearance information, work addresses, including division/group, work email addresses and work telephone numbers of the Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), General Counsel, and the Corporate Security Officer (CSO) or Facility Security Officer (FSO), or their equivalents. DIB participants also provide POC information for personnel responsible for the implementation and execution of the DIB CS/IA program within their company (e.g., may include policy and technical personnel that will interact with DoD).

Affected Public: Business or other for-profit and not-for-profit institutions participating in the voluntary DIB CS/IA program.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

(b) Title: *DIB Cyber Security/Information Assurance Cyber Incident Reporting*

Type of Request: New.

Phased expansion of DIB CS/IA Number of Participants increases to 750 over three years.

Projected Responses Per Participant: 5

Annual Responses: Year 1 responses are 1,250. Year 2 responses are 2,500. Year 3 responses are 3,750.

Average Burden Per Response: 7 hours (this includes searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information).

Annual Burden Hours: Year 1 burden hours are 8,750 hours. Year 2 burden hours are 17,500 hours. Year 3 burden hours are 26,250 hours.

Needs and Uses: The collection of this information is necessary to enhance and supplement DIB participants' information security capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The requested information supports the information assurance objectives, cyber threat information sharing, and incident reporting between DoD and the DIB participants. In most cases, DIB participants report incidents using a DIB CS/IA standardized Incident Collection Form (ICF). In some cases, a company may elect to

report the incident without using the ICF; and companies may report incidents through a variety of communications channels, including email, fax, or by phone, if necessary.

Affected Public: Business or other for-profit and not-for-profit institutions participating in the DIB CS/IA program.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

OMB Desk Officer:

Written comments and recommendations on the information collection should be sent to Ms Jasmeet Seehra at the Office of Management and Budget, DoD Desk Officer, Room 10102, New Executive Office Building, Washington, DC 20503, with a copy to the Director, DIB CS/IA Program Office, at the Office of the DoD Chief Information Officer, 6000 Defense Pentagon, Attn: DIB CS/IA Program Office, Washington, D.C. 20301, or email at DIB.CS/IA.Reg@osd.mil. Comments can be received from 30 to 60 days after the date of this notice, but comments to OMB will be most useful if received by OMB within 30 days after the date of this notice. You may also submit comments, identified by docket number and title, by the following method: *Federal Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the

Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

To request more information on this information collection or to obtain a copy of the proposal and associated collection instruments, please write to Director, DIB CS/IA Program Office, at Office of the DoD Chief Information Officer, Attn: DIB CS/IA Program Office, 6000 Defense Pentagon, Washington, D.C. 20301.

Executive Order 13132, “Federalism”

It has been certified that 32 CFR part 236 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

- (a) The States;
- (b) The relationship between the National Government and the States; or
- (c) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 236

Contracts, Security measures

Accordingly 32 CFR Part 236 is added to read as follows:

**PART 236– DEPARTMENT OF DEFENSE (DOD)-DEFENSE INDUSTRIAL BASE
(DIB) VOLUNTARY CYBER SECURITY AND INFORMATION ASSURANCE (CS/IA)
ACTIVITIES**

236.1 Purpose.

236.2 Definitions.

236.3 Policy.

236.4 Procedures.

236.5 Cyber Security Information Sharing.

236.6 General Provisions.**236.7 DIB Participant Eligibility Requirements.**

Authority: 10 U.S.C. § 2224; 44 U.S.C. § 3506; 44 U.S.C. § 3544.

236.1 Purpose.

Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. DoD's voluntary DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

236.2 Definitions.

As used in this part:

- (a) *Advanced persistent threat* means an extremely proficient, patient, determined, and capable threat.
- (b) *Attribution information* means information that identifies the DIB participant, whether directly or indirectly, by the grouping of information that can be traced back to the DIB participant (e.g., program description, facility locations).
- (c) *Compromise* means disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional, or unintentional, disclosure, modification, destruction, loss of an object, or the copying of information to unauthorized media may have occurred.
- (d) *Covered defense information* means unclassified information that:
 - (1) Is:
 - (i) Provided by or on behalf of the DoD to the DIB participant; or

(ii) Collected, developed, received, transmitted, used, or stored by the DIB participant in support of an official DoD activity; and

(2) Is:

(i) Technical information marked for restricted distribution in accordance with DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," or DoD Directive 5230.24, "Distribution Statements on Technical Documents";

(ii) Information subject to export control under the International Traffic in Arms Regulations (ITAR) (http://pmdtc.state.gov/regulations_laws/itar_official.html) , or the Export Administration Regulations (EAR) .(<http://ecfr.gpoaccess.gov>, Title 15, part 730);

(iii) Information designated as Critical Program Information (CPI) in accordance with DoD Instruction 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense";

(iv) Information that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries as described in 5205.02-M, "DoD Operations Security (OPSEC Program Manual";

(v) Personally Identifiable Information (PII) that can be used to distinguish or trace an individual's identify in accordance with DoD Directive 5400.11, "DoD Privacy Program";

(vi) Information bearing current and prior designations indicating unclassified controlled information (e.g., For Official Use Only, Sensitive But Unclassified, and Limited Official Use, DoD Unclassified Controlled Nuclear Information, Sensitive Information) that has not been cleared for public release in accordance with DoD Directive 5230.29, "Clearance of DoD Information for Public Release" (see also Appendix 3 of DoD 5200.1-R, "Information Security Program Regulation"); or

(vii) Any other information that is exempt from mandatory public disclosure under DoD Directive 5400.07, “DoD Freedom of Information Act (FOIA) Program”, and DoD Regulation 5400.7-R, “DoD Freedom of Information Program”.

(e) *Covered DIB systems* means an information system that is owned or operated by or for a DIB participant and that processes, stores, or transmits covered defense information.

(f) *Cyber incident* means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein..

(g) *Cyber intrusion damage assessment* means a managed, coordinated process to determine the effect on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from compromise of a DIB participant’s unclassified computer system or network.

(h) *Defense Industrial Base (DIB)* means the Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

(i) *DIB participant* means a cleared defense contractor that has met all of the eligibility requirements to participate in the voluntary DIB CS/IA information sharing program as set forth in this part.

(j) *Government* means the United States Government.

(k) *Government Furnished Information (GFI)* means information provided by the Government under the voluntary DIB CS/IA program, including but not limited to cyber threat information and information assurance practices.

(l) *Information* means any communication or representation of knowledge such as facts, data, or

opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(m) *Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(n) *Threat* means any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

236.3 Policy.

It is DoD policy to:

(a) Establish a comprehensive approach for enhancing and supplementing DIB information assurance capabilities to safeguard covered defense information on covered DIB systems.

(b) Increase the Government and DIB situational awareness of the extent and severity of cyber threats, including in support of U.S. critical infrastructure and key resources.

236.4 Procedures.

(a) The Government and each DIB participant will execute a voluntary standardized agreement, referred to as a Framework Agreement (FA), to share, in a timely and secure manner, on a recurring basis, and to the greatest extent possible, cyber security information relating to information assurance for covered defense information on covered DIB systems.

(b) Each such FA between the Government and a DIB participant must comply with and implement the requirements of this part, and will include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in this part with individual DIB participants.

(c) The Government operational focal point for cyber security information sharing under the DIB CS/IA program is the DoD Cyber Crime Center (DC3) DoD-DIB Collaborative Information Sharing Environment (DC3/DCISE).

(d) The Government will maintain a website or other internet-based capability to provide potential DIB participants with information about eligibility and participation in the program, to enable the online application or registration for participation, and to support the execution of necessary agreements with the Government.

(e) Prior to receiving GFI from the Government, each DIB participant shall provide the requisite points of contact information, to include security clearance and citizenship information, for the designated personnel within their company (e.g., typically 3-10 company designated points of contact) in order to facilitate the DoD-DIB interaction in the DIB CS/IA program..

(f) GFI will be issued via both unclassified and classified means. DIB participant handling and safeguarding of classified information shall be in compliance with the Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB participants of any revisions to previously specified transmission or procedures.

(g) Except as authorized in this part or in writing by the Government, DIB participants may (1) use GFI to safeguard covered defense information only on covered DIB systems that are U.S. based (i.e., provisioned, maintained, or operated within the physical boundaries of the United States); and (2) share GFI only within their company or organization, on a need to know basis, with distribution restricted to U.S. citizens (i.e., a person born in the United States, or naturalized, holding a U.S. passport). However, in individual cases, upon request of a DIB participant that has determined that it requires the ability to share the information with a non U.S.

citizen, or to use the GFI on a non-U.S. based covered DIB system, and can demonstrate that appropriate information handling and protection mechanisms are in place, the Government may authorize such disclosure or use under appropriate terms and conditions.

(h) DIB participants shall maintain the capability to electronically disseminate GFI within the Company in an encrypted fashion (e.g., using Secure/Multipurpose Internet Mail Extensions (S/MIME), secure socket layer (SSL), DoD-approved medium assurance certificates).

(i) The DIB participants shall not share GFI outside of their company or organization, regardless of personnel clearance level, except as authorized in this part or otherwise authorized in writing by the Government.

(j) If the DIB participant utilizes a third-party service provider (SP) for information system security services, the DIB participant may share GFI with that SP under the following conditions and as authorized in writing by the Government:

(1) The DIB participant must identify the SP to the Government and request permission to share or disclose any GFI with that SP (which may include a request that the Government share information directly with the SP on behalf of the DIB participant) solely for the authorized purposes of this program;

(2) The SP must provide the Government with sufficient information to enable the Government to determine whether the SP is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI;

(3) Upon approval by the Government, the SP must enter into a legally binding agreement with the DIB participant (and also an FA with the Government in any case in which the SP will receive or share information directly with the Government on behalf of the DIB participant) under which the SP is subject to all applicable requirements of this part and of any supplemental

terms and conditions in the DIB participant's FA with the Government, and which authorizes the SP to use the GFI only to provide information security services for the DIB participant's covered DIB systems, and not for any other purpose.

(k) The DIB participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services. However, this does not prohibit a DIB participant from being designated an SP in accordance with paragraph (j).

236.5 Cyber Security Information Sharing.

(a) *GFI*. The Government shall share GFI with DIB participants under the DIB CS/IA program.

(b) *Initial Incident Reporting*. The DIB participant shall report to DC3/DCISE cyber incidents involving covered defense information on a covered DIB system within 72 hours of discovery. DIB participants also may report other cyber incidents if the DIB participant determines the incident may be relevant to information assurance for covered defense information or covered DIB systems.

(c) *Follow-up Reporting*. After an initial incident report, the Government and the DIB participant may voluntarily share additional information that is determined to be relevant to a reported incident, including information regarding forensic analyses, mitigation and remediation, and cyber intrusion damage assessments.

(d) *Cyber Intrusion Damage Assessment*. Following analysis of a cyber incident, DC3/DCISE may provide information relevant to the potential or known compromise of DoD acquisition program information to the Office of the Secretary of Defense's Damage Assessment Management Office (OSD DAMO) for a cyber intrusion damage assessment. The Government may provide DIB participants with information regarding the damage assessment.

(e) *Attribution Information.* The Government shall take reasonable steps to protect against the unauthorized release of attribution information and other nonpublic information received from a DIB participant (or derived from such information provided by a DIB participant) under the DIB CS/IA program, including applicable exemptions under the Freedom of Information Act (5 U.S.C. 552). The Government will restrict its internal use and disclosure of attribution information to only those authorized Government personnel and Government support contractors that are bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information.

(f) *Non-Attribution Information.* The Government may share non-attribution information that was provided by a DIB participant (or derived from information provided by a DIB participant) with other DIB participants in the DIB CS/IA program, and may share such information throughout the Government (including with Government support contractors that are bound by appropriate confidentiality obligations) for cyber security and information assurance purposes for the protection of Government information or information systems.

(g) *Electronic Media.* Electronic media/files provided by DIB participants are maintained by the digital and multimedia forensics laboratory at DC3, which implements specialized handling procedures to maintain its accreditation as a digital and multimedia forensics laboratory. DC3 will maintain, control, and dispose of all electronic media/files provided by DIB participants for incident response and analysis in accordance with established DoD policies and procedures.

236.6 General Provisions.

(a) Confidentiality of information that is exchanged under this program will be protected to the maximum extent authorized by law, regulation, and policy.

(b) The Government and DIB participants will conduct their respective activities under this program in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. The Government and the DIB participant each bear responsibility for their own actions under this program.

(c) Prior to sharing any information with the Government under this program, the DIB participant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements. The Government may request from any DIB participant additional information or assurances regarding such DIB participant's policies or practices, or the determination by the DIB participant that such policies or practices comply with applicable legal requirements.

(d) This voluntary DIB CS/IA program is intended to safeguard covered defense information. None of the restrictions on the Government's use or sharing of information under the DIB CS/IA program shall limit the Government's ability to conduct law enforcement or counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements.

(e) Participation in the DIB CS/IA program is voluntary and does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(f) A DIB participant's voluntary participation in this program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to

provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(g) The DIB participant and the Government may each unilaterally limit or discontinue participation in this program at any time. Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program, as required by law, regulation, contract, or the FA.

(h) Upon termination of the FA, and/or change of Facility Security Clearance status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(i) Participation in this program does not abrogate the Government's or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation.

236.7 DIB Participant Eligibility Requirements.

To be eligible to participate in this program, a DIB participant must execute the standardized FA with the Government, including compliance with requirements applicable to DIB participants as set forth in sections 236.4 through 236.6 of this part. In addition, the DIB Participant must:

(a) Have or acquire DoD-approved medium assurance certificates to enable encrypted unclassified information sharing between the Government and DIB participants;

(b) Have an existing active Facility Security Clearance (FCL) granted under the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M) with approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding

(<http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>);

(c) Have or acquire a Communications Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4; and

(d) Obtain access to DoD's secure voice and data transmission systems supporting the DIB CS/IA program.

DATED:

PATRICIA L. TOPPINGS

OSD Federal Register

Liaison Officer

Department of Defense

Fact Sheet: Defense Industrial Base (DIB) Cyber Security/Information Assurance Program and DIB Enhanced Cybersecurity Services

The United States continues to face a significant risk that critical Defense information residing on DIB networks and systems can be compromised by malicious cyber actors resulting in potential economic losses or damage to United States national security. The Department of Defense is actively engaged in multiple efforts to foster mutually beneficial partnerships with the Defense Industrial Base (DIB) to protect Department of Defense information residing on or passing through DIB systems. One such effort is the DIB Cyber Security/Information Assurance (CS/IA) Program, including its optional Enhanced Cybersecurity Services (ECS) component.

Bilateral Information Sharing

The DIB CS/IA Program is designed to improve DIB network defenses and allows DIB companies and the Government to reduce damage to critical programs when defense information is compromised. The DIB CS/IA Program includes a voluntary information sharing component under which DIB companies and the Government agree to share cyber security information out of a mutual concern for the protection of sensitive but unclassified information related to DoD programs on DIB company networks.

Under the DIB CS/IA Program, DoD provides participating DIB Companies with unclassified indicators and related, classified contextual information. DIB companies can choose whether to incorporate the indicators into their own traffic screening or other security tools, and they can review or act on the contextual information as they wish to better address the cybersecurity threats they face. DoD also shares mitigation measures to assist DIB Companies' cybersecurity efforts.

DIB companies also report known intrusion events to the Government and may participate in Government damage assessments, if needed. A DIB company may report any cybersecurity event that may be of interest to the cyber community, at its discretion.

Enhanced Cyber Security Services (ECSS)

As an additional and optional part of the program, the Government will furnish classified threat and technical information to voluntarily participating DIB Companies or their Commercial Service Providers (CSPs). This sensitive Government furnished information enables the DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of known malicious activity and to further protect Department of Defense program information. Any CSPs that are capable of implementing the Government furnished information in compliance with security requirements are eligible to participate and offer the cybersecurity services to participating DIB companies. CSPs may also charge for providing this service to participating DIB companies.

DIB Company Participation

To participate in the DIB CS/IA Program, eligible DIB companies sign a Framework Agreement with DoD. Once in the DIB CS/IA Program, a DIB company may also elect to participate in the ECS component in several different ways: by meeting the security requirements to implement the countermeasures on its own networks, by purchasing the services from a participating CSP, or by meeting the requirements to become a CSP to offer the services to other DIB companies.

The DIB CS/IA Program is open to all eligible DIB companies. The content, manner, and means by which DIB companies participate are captured in a Framework Agreement between DoD and the DIB company. More information, including eligibility requirements, is available in the Federal Register [[link](#)], and on the DIB CS/IA Program public website (<http://dibnet.dod.mil/>).



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities

DoD CIO

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

Yes, DITPR Enter DITPR System Identification Number

Yes, SIPRNET Enter SIPRNET Identification Number

No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

Yes

No

If "Yes," enter UPI

007-97-05-08-02-3915-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

Yes

No

If "Yes," enter Privacy Act SORN Identifier

In process

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

April 28, 2011

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

In process

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Department of Defense (DoD) Instruction (DoDI) 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, directs the conduct of DIB CS/IA activities to protect unclassified DoD information that transits, or resides on, unclassified DIB information systems and networks. DoD Directive (DoDD) 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, addresses the responsibilities of DC3, including its electronic and multimedia forensics laboratory, which is accredited by the American Society of Crime Laboratory Directors Laboratory Accreditation Board; collaboration with U.S. Government (USG) and private industry organizations; and designates DC3 as the information sharing focal point for the DIB CS/IA program. These activities, including the collection, management and sharing of information for cyber security purposes, support and implement national and DoD-specific guidance and authority, including the following:

1. Information Assurance (IA):

DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of title 10, U.S. Code (U.S.C.), requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis. (10 U.S.C. § 2224(a)). The program must provide continuously for the availability,

integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure. (10 U.S.C. § 2224(b)). The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations. (10 U.S.C. § 2224(c)). The program must provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems. (10 U.S.C. § 2224(d)).

The Defense IA Program also must ensure compliance with federal IA requirements provided in the Federal Information Security Management Act (FISMA). (44 U.S.C. §§ 3541 et seq.). FISMA requires all federal agencies to provide information security protections for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. (44 U.S.C. § 3544(a)(1)(A)). Agencies are expressly required to develop, document, and implement programs to provide information security for information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source. (44 U.S.C. § 3544(b)).

2. Critical Infrastructure Protection (CIP):

Under Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," the Department of Homeland Security (DHS) leads the national effort to protect public and private critical infrastructure. (HSPD-7, ¶(7)). This includes coordinating implementation activities between federal agencies, state and local authorities, and the private sector. Regarding cyber security, these efforts are to include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. (HSPD-7, ¶(12)).

The Department of Defense is the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB) sector (HSPD-7, ¶(18)(g)), and thus engages with the DIB on a wide range of CIP matters, including but not limited to cyber security. HSPD-7 charges the SSAs to: collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. (HSPD-7, ¶(19)). More specifically, regarding coordination with the private sector, HSPD-7 provides that DHS and the SSAs "will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms [to] identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." (HSPD-7, ¶(25)). Within DoD, CIP is implemented by DoDD 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, and DoDI 3020.45, "Defense Critical Infrastructure Program (DCIP) Management" April 21, 2008.

3. Comprehensive National Cybersecurity Initiative:

National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD) 23, which formalizes the Comprehensive National Cyber Security Initiative (CNCI), directs each Department to improve situational awareness between the Government and private sector regarding the extent and severity of the cyber threat. Under CNCI, the Department of Homeland Security (DHS), in consultation with the heads of other SSAs, including DoD, submitted the "Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships." This report recommends implementing real-time cyber situational awareness and promoting public-private cyber information sharing efforts. Furthermore, the "Cyberspace Policy Review" (also known as the 60-Day Review), released by the President on May 29, 2009, identifies cyber security as a top priority of the administration. The report specifically recommends accelerating private-sector network incident reporting to the Government. The "International Strategy for Cyberspace," released by the President in

May 2011, emphasizes the need for public and private sector partnership to strengthen networks and systems and make steady progress towards shared situational awareness of network vulnerabilities.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The information systems and information collection activities covered by this PIA are used to support key elements of the Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program (see DoD Instruction (DoDI) 5205.13, "[DIBCS/IA] Activities," January 29, 2010), to protect unclassified DoD information that transits, or resides, on unclassified DIB information systems and networks. This includes support provided by the DIB CS/IA Program Office, the DoD Cyber Crime Center (DC3) and other government stakeholders.

More specifically, this PIA covers a voluntary cyber security information sharing activity between the DoD and DIB companies. In general, DoD provides cyber threat information and information assurance (IA) best practices to DIB companies to help them better protect their unclassified networks to protect DoD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents to the DoD-DIB Collaborative Information Sharing Environment (DCISE), located at DC3. The DoD analyzes the information reported by the DIB company regarding any such cyber incident, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures. In addition to this initial reporting and analysis, the DoD and DIB company may pursue, on a voluntary basis, follow-on, more detailed, digital forensics analysis or damage assessments, including sharing of additional electronic media/ files or information regarding the incident or the affected systems, networks, or information. The information sharing arrangements between the DoD and each participating DIB company is memorialized in a standardized bilateral Framework Agreement (FA).

Such DoD-DIB cyber security information sharing practices are under continuous review and improvement, including the development and testing of additional information sharing mechanisms and models. For example, the new DIB Exploratory Cybersecurity Initiative (also known as the "Exploratory Pilot" or "Opt-In Pilot"), builds on the existing DIB CS/IA Program and FAs, serving as a short-term proof-of-concept demonstration in which DoD would share cyber threat information and technical information directly with commercial providers of internet, network, and communications services providers. In this sharing model, the commercial service providers are authorized to use the DoD-provided information to further protect participating DIB company networks, which allows the DIB companies the option of acquiring such protections from a commercial provider, rather than each DIB company independently deploying the information directly on its own networks. This Exploratory Pilot utilizes all of the incident reporting, forensics analysis, and damage assessment procedures already established under the DIB CS/IA program and FAs, and thus the sharing of PII for the Exploratory Pilot is also covered by this PIA.

Although these DIB CS/IA Program information sharing activities are focused on sharing cyber security related information, the operational implementation of this sharing arrangement involves sharing and managing PII in two supporting ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) although it is not typical or expected, there is always the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to or embedded within the cyber security information being shared. Each of these circumstances is discussed in more detail below:

1. DIB CS/IA Program Administration and Management:

As part of the administrative management of the DIB CS/IA Program's information sharing activities, each participating DIB company provides basic identifying information for a limited number of its personnel who are authorized to serve as the primary company points of contact (POCs). The information provided for each POC includes routine business contact information (e.g., name, title, organizational unit, business email and phone), plus additional information necessary to verify the individual's authorization to receive classified information or controlled unclassified information (e.g., security clearance, citizenship). This information is required by the DIB CS/IA program office to manage the program and interact with the companies through

routine emails, phone calls, and participation in periodic classified meetings. A DIB company that is not yet participating in the Program may also provide POC information to the DIB CS/IA Program office in order to discuss Program application procedures or related information regarding the Program.

In addition to the designation of a limited number of primary POCs for the DIB company's overall participation in the DIB CS/IA Program, additional POC information may be provided in the individual incident reports submitted by the company. In most cases, the DIB companies report incidents using a DIB CS/IA Program standardized Incident Collection Form (ICF), which is submitted as the initial incident report to the DoD-DIB Collaborative Information Sharing Environment (DCISE) at DC3. The ICF includes the basic POC information (e.g., name, organizational unit, business email and phone) for the DIB company representative who is submitting the initial report. The ICF also allows the reporting company to provide the same basic POC information for other company personnel that are knowledgeable about, or otherwise relevant for, the reported incident (e.g., POCs for incident response, technical issues, or the affected business unit). In some cases, a company may elect to report the incident without using the ICF; and companies may report incidents through a variety of communications channels, including email, fax, or by phone, if necessary.

Collecting this type of POC information is the only element of this information sharing activity in which the DIB CS/IA program intentionally collects PII; however, there are other portions of the information sharing activities that present the potential for the DIB companies to provide DoD with PII that is incidental to, or embedded within, other cyber security information being shared—resulting in an inadvertent collection of PII.

2. Cyber Incident Response and Analysis:

Although it is not typical or expected, it is nevertheless possible that a DIB company may voluntarily submit PII to DoD in connection with the initial cyber incident reporting or response activities, or during follow-up digital forensics or damage assessment activities. Accordingly, the Program is designed to provide appropriate handling and safeguards in the event that PII is (inadvertently) collected in these circumstances.

For example, when providing the initial incident report on the ICF, the DIB company provides a description of the cyber incident, including technical and contextual details regarding any or all relevant aspects of the incident. In some cases, the DIB company may determine that PII, or what appears to be PII, is relevant in describing the event (e.g., an individual's name and email address that may be spoofed in connection with an email phishing attempt or an email used as the delivery mechanism for malware). The ICF allows the company to describe the incident in two levels of detail and sensitivity: (i) a fully detailed version that may contain attribution or other sensitive information (e.g., PII) that is provided for internal DCISE use; and (ii) an alternative description that provides only such information that the company authorizes to be released outside the DCISE for cyber security purposes. Subsequently, the DCISE also follows up with the DIB company to confirm the nature and extent of information that the DIB company authorizes for release outside the DCISE for cyber security purposes.

In addition, the DIB company also may voluntarily share PII during the digital forensics analysis or damage assessment activities following the initial incident response. Or, more accurately, a DIB company may determine that it is not necessary to redact or withhold certain types of PII from the information that it is otherwise voluntarily sharing for these follow-on analyses. The DoD and DIB companies recognize that in some cases, after the initial incident report and preliminary investigation, a more complete analysis of the event may be necessary. On a voluntary basis, DIB companies may share additional information about potentially compromised information systems with the DoD for this purpose. DIB companies may elect to limit the nature and extent of information shared, due to legal, contractual, or other restrictions.

Similarly, as part of the follow-up for each reported incident, the DIB company reviews the potentially compromised systems or networks and reports to DoD regarding the presence of files or information associated with DoD programs, systems, or military applications. When the reported cyber intrusion affects systems containing such DoD information, the DIB companies will preserve and share with DoD the unclassified files on threat-accessed systems that pertain to Government programs, unless there are legal or contractual reasons that preclude sharing (e.g., the images may contain PII or third-party proprietary information that are subject to nondisclosure prohibitions). The DoD's Damage Assessment Management Office (DAMO), an organizational element of the Under Secretary of Defense for Acquisition, Technology and Logistics, reviews the available information to determine whether a more complete damage assessment is warranted.

These information sharing mechanisms are intended to enhance a participating DIB company's ability to detect and defend against cyber intrusions and other malicious activity occurring on their networks, in order to better protect Defense information. In doing so, the DIB CS/IA Program has established procedures designed to ensure that the DIB companies share information with DoD only if it is relevant to the forensics or damage assessment analysis, and only after the DIB company verifies that it is authorized to share the information with the DoD for these purposes.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

There are minimal risks associated with the PII collected in connection with the DoD-DIB cyber security information sharing activities under the DIB CS/IA Program, and risks are effectively addressed to safeguard privacy:

- The PII received by the DoD is provided voluntarily by authorized DIB company representatives, subject to mutually agreed upon restrictions (e.g., in the FA);
- The nature of the PII being intentionally collected is limited to ordinary business contact information;
- Once collected, access and use of PII is strictly limited to authorized personnel that need the information for cyber security purposes;
- All personnel receiving access to the collected PII are required to undergo training and are subject to appropriate nondisclosure restrictions; and
- The PII is maintained for only so long as necessary for DIB CS/IA Program activities, and is managed and disposed of in accordance with applicable records management requirements.

Additional details regarding these risk mitigations and safeguards are discussed below.

The DIB CS/IA information sharing activities covered by this PIA are focused on sharing cyber security related information, and thus the Program seeks to minimize the collection and management of PII except as necessary to support the program. The operational implementation of this sharing arrangement involves sharing and managing PII in two supporting or incidental ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) for cyber incident response and analysis purposes, although it is not typical or expected, there exists the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for the cyber security analysis. Details on the nature and circumstances of PII collection for these purposes is discussed in more detail in Section 2. g.(1) above.

As discussed previously, the DIB CS/IA Program intentionally collects PII regarding DIB company POCs only for routine program administration and management purposes. This PII does not involve any particularly sensitive personal information – it is limited to the individual's typical business contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone), as well as other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program.

Although this basic POC information may not be a particularly sensitive type of PII, it is nevertheless tightly controlled within the DIB CS/IA Program – in the same manner and for the similar purposes, that the Program controls DIB company “attribution information” (i.e., information that identifies a company or its programs, whether directly or indirectly, by the grouping of information that can be traced back to that company). Although the name of a DIB company or its programs, or the basic contact information for the company's POCs, might not ordinarily be considered particularly sensitive, the association of that company or its specific POCs with particular cyber security activities, or with particular cyber security incidents, may be extremely sensitive, closely guarded information. Accordingly, the DIB CS/IA Program restricts access to such PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. For example, all USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

DC3 will maintain, control, and dispose of all media provided by DIB companies in accordance with established policies and procedures for the digital and multimedia forensics laboratory. The media are protected using procedural controls that are the same as, or similar to, those DC3 uses to handle evidence that it processes as part of criminal investigations. Access to the media containing files that may have PII, is strictly controlled and limited to those participating in formal DIB cyber intrusion damage assessments. The media are maintained by the digital and multimedia forensics laboratory, an accredited facility. The files and media do not leave DC3 – physically or electronically.

The Program's information sharing procedures are designed to ensure the DIB companies share information with DoD only if it is relevant to cyber intrusion incidents or follow-on forensics or cyber intrusion damage assessment analysis. When sharing electronic images or files with the DoD for forensics or damage assessment activities, the DIB companies will identify the types of sensitive information (e.g., PII, proprietary, export controlled) that may be contained in the shared files. However, when the DoD is performing its analysis on the files, it may discover PII (or other sensitive information) that had not been identified by the DIB company when the information was submitted. If this occurs, all investigative work ceases, the DIB company is notified that PII (or sensitive information) was discovered, and the DIB company provides guidance in writing as to how it would like to proceed (e.g., cease forensics analysis and return the electronic media to the DIB company for further review to verify the company's authorization to share that information with DoD for cyber security activities).

- How long will any collected PII be stored, and how will such PII be disposed of?

The DIB company POC information provided to support the DIB CS/IA administration and management process is maintained only so long as the designated points of contact represent the participating company. When the DIB CS/IA program office is notified that the DIB Company personnel are being replaced, the POC information databases are updated and outdated PII is archived in accordance with records management requirements.

Inadvertently collected PII that may be submitted by DIB companies in connection with incident reporting and response is maintained, controlled, and disposed of when no longer needed for intrusion investigation, forensics analysis, and damage assessment activities. The time it takes to complete a cyber intrusion forensics analysis and damage assessment will vary. Some of the assessments will be more complex and require more time than others. DC3 will dispose of media when no longer needed, as it does with DoD information it reviews as part of criminal investigations.

In all cases, the management and disposal of this information will comply with all applicable DoD records management procedures and requirements, and records disposition schedules.

- What compliance or oversight mechanisms are used to ensure that PII is protected?

DC3 has detailed procedures and processes in place to control access to inadvertently collected PII. These processes capitalize on the procedures DC3 has in place in its law enforcement capacity. The same strict need-to-know standard and chain of custody process used to handle evidence are used to control files and media provided by DIB companies. All personnel with access to DIB company submitted materials are required to undergo training and then sign a DIB CS/IA Program standardized NDA before being granted access to any information. The NDAs are maintained by DC3 and no access is given to the files unless an NDA has been executed and is on file with DC3.

The DIBCS/IA Program Office, and DC3, also coordinate with the Defense Privacy and Civil Liberties Office to ensure that the program practices and procedures comply with applicable requirements concerning appropriate management and protection of PII, and privacy and civil liberties considerations.

- Will the networks that store or process the PII be monitored? How would participating entities know that their networks are subject to monitoring?

None of these DIB CS/IA activities involve any DoD or USG personnel performing any monitoring of DIB company or other private networks. The DIB companies are responsible for the conduct of any monitoring of their own networks. The only PII received by DoD under these activities is PII that is provided directly to DoD by authorized DIB company personnel. Once any such PII is received in DoD systems or networks, the

DoD monitoring policies and practices are applicable; including DoD-wide requirements for system logon banners and user agreements that operate to ensure legally effective user notice and consent to DoD monitoring (see Directive Type Memorandum 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," May 8, 2008).

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)?
Indicate all that apply.

Within the DoD Component.

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is not shared (physically or electronically) outside of DC3 facilities. Information and media are maintained at DC3 with strict accountability and need-to-know on those USG and DoD contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

Other DoD Components.

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is not shared (physically or electronically) outside of DC3 facilities. Information and media are maintained at DC3 with strict accountability and need-to-know on those USG and DoD contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

Other Federal Agencies.

Specify.

PII is not shared with other federal agencies, except in support of authorized law enforcement or counterintelligence activities. In any other case, DoD would obtain the appropriate permission (e.g., from the DIB company or the individual identified by the PII) for any other sharing with another Federal agency. In some cases, the DIB company may determine that PII, or what appears to be PII, is relevant in describing the event (e.g., an individual's name and email address that may be spoofed in connection with an email phishing attempt, or an email used as the delivery mechanism for malware). Only such PII as authorized by the company will be released outside of the DoD.

State and Local Agencies.

Specify.

- Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is not shared (physically or electronically) outside of DC3 facilities. Information and media are maintained at DC3 with strict accountability and need-to-know on those USG and DoD contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information. In some cases, the DIB company may determine that PII, or what appears to be PII, is relevant in describing the event (e.g., an individual's name and email address that may be spoofed in connection with an email phishing attempt, or an email used as the delivery mechanism for malware). Only such PII authorized by the company will be released to a contractor.

- Other** (e.g., commercial providers, colleges).

Specify.

In any other case, DoD would not share the PII except after obtaining the appropriate permission (e.g., from the DIB company or the individual identified by the PII).

i. Do individuals have the opportunity to object to the collection of their PII?

- Yes** **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she can object to the collection of PII at that time.

(2) If "No," state the reason why individuals cannot object.

DIB company POC information may also be intentionally collected from a DIB company representative that is providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to object at this point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she is provided the opportunity to consent or not consent to specific uses of PII when they are presented with a Privacy Act Statement.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DIB company POC information may also be intentionally collected from a DIB company representative that is providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to consent or withhold consent for specific uses at the point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement Privacy Advisory
 Other None

Describe each applicable format.

Privacy Act Statement to include the authorities to collect the information; the purpose or purposes for which the information is to be used; the routine uses that will be made of the information; whether providing the information is voluntary or mandatory and the effects on the individual if he or she chooses not to provide the requested information.

--

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities
DoD CIO

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

In process

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Department of Defense (DoD) Instruction (DoDI) 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, directs the conduct of DIB CS/IA activities to protect unclassified DoD information that transits, or resides on, unclassified DIB information systems and networks. DoD Directive (DoDD) 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, addresses the responsibilities of DC3, including its electronic and multimedia forensics laboratory, which is accredited by the American Society of Crime Laboratory Directors Laboratory Accreditation Board; collaboration with U.S. Government (USG) and private industry organizations; and designates DC3 as the information sharing focal point for the DIB CS/IA program. These activities, including the collection, management and sharing of information for cyber security purposes, support and implement national and DoD-specific guidance and authority, including the following:

1. Information Assurance (IA):

DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of title 10, U.S. Code (U.S.C.), requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis. (10 U.S.C. § 2224(a)). The program must provide continuously for the availability,

integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure. (10 U.S.C. § 2224(b)). The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations. (10 U.S.C. § 2224(c)). The program must provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems. (10 U.S.C. § 2224(d)).

The Defense IA Program also must ensure compliance with federal IA requirements provided in the Federal Information Security Management Act (FISMA). (44 U.S.C. §§ 3541 et seq.). FISMA requires all federal agencies to provide information security protections for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. (44 U.S.C. § 3544(a)(1)(A)). Agencies are expressly required to develop, document, and implement programs to provide information security for information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source. (44 U.S.C. § 3544(b)).

2. Critical Infrastructure Protection (CIP):

Under Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," the Department of Homeland Security (DHS) leads the national effort to protect public and private critical infrastructure. (HSPD-7, ¶(7)). This includes coordinating implementation activities between federal agencies, state and local authorities, and the private sector. Regarding cyber security, these efforts are to include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. (HSPD-7, ¶(12)).

The Department of Defense is the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB) sector (HSPD-7, ¶(18)(g)), and thus engages with the DIB on a wide range of CIP matters, including but not limited to cyber security. HSPD-7 charges the SSAs to: collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. (HSPD-7, ¶(19)). More specifically, regarding coordination with the private sector, HSPD-7 provides that DHS and the SSAs "will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms [to] identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." (HSPD-7, ¶(25)). Within DoD, CIP is implemented by DoDD 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, and DoDI 3020.45, "Defense Critical Infrastructure Program (DCIP) Management" April 21, 2008.

3. Comprehensive National Cybersecurity Initiative:

National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD) 23, which formalizes the Comprehensive National Cyber Security Initiative (CNCI), directs each Department to improve situational awareness between the Government and private sector regarding the extent and severity of the cyber threat. Under CNCI, the Department of Homeland Security (DHS), in consultation with the heads of other SSAs, including DoD, submitted the "Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships." This report recommends implementing real-time cyber situational awareness and promoting public-private cyber information sharing efforts.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The information systems and information collection activities covered by this PIA are used to support key elements of the Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program (see DoD Instruction (DoDI) 5205.13, "[DIBCS/IA] Activities," January 29, 2010), to protect unclassified DoD information that transits, or resides, on unclassified DIB information systems and networks. This includes support provided by the DIB CS/IA Program Office, the DoD Cyber Crime Center (DC3), the Damage Assessment Management Office (DAMO), and other government stakeholders.

More specifically, this PIA covers a voluntary cyber security information sharing activity between the DoD and DIB companies. In general, DoD provides cyber threat information and information assurance (IA) best practices to DIB companies to help them better protect their unclassified networks to protect DoD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents to the DoD-DIB Collaborative Information Sharing Environment (DCISE), located at DC3. The DoD analyzes the information reported by the DIB company regarding any such cyber incident, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures. In addition to this initial reporting and analysis, the DoD and DIB company may pursue, on a voluntary basis, follow-on, more detailed, digital forensics analysis or damage assessments, including sharing of additional electronic media/ files or information regarding the incident or the affected systems, networks, or information. The information sharing arrangements between the DoD and each participating DIB company are memorialized in a standardized bilateral Framework Agreement (FA).

Such DoD-DIB cyber security information sharing practices are under continuous review and improvement, including the development and testing of additional information sharing mechanisms and models. For example, the new DIB Exploratory Cybersecurity Initiative (also known as the "DIB Cyber Pilot"), builds on the existing DIB CS/IA Program and FAs, serving as a short-term proof-of-concept demonstration in which DoD would share cyber threat information and technical information directly with commercial providers of internet, network, and communications services providers. In this sharing model, the commercial service providers (CSPs) enter into a modified version of the FA that authorizes them to use the DoD-provided information to further protect participating DIB company networks. This modified information sharing model allows the DIB companies the option of acquiring such additional cyber security protections from commercial providers, rather than each DIB company independently deploying the information directly on its own networks. This Pilot utilizes all of the incident reporting, forensics analysis, and damage assessment procedures already established under the DIB CS/IA program and FAs, and thus the sharing of PII for the Exploratory Pilot is also covered by this PIA.

Although these DIB CS/IA Program information sharing activities are focused on sharing cyber security related information, the operational implementation of this sharing arrangement involves sharing and managing PII in two supporting ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) although it is not typical or expected, there is always the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to or embedded within the cyber security information being shared. Each of these circumstances is discussed in more detail below:

1. DIB CS/IA Program Administration and Management:

As part of the administrative management of the DIB CS/IA Program's information sharing activities, each participating DIB company provides basic identifying information for a limited number of its personnel who are authorized to serve as the primary company points of contact (POCs). The information provided for each POC includes routine business contact information (e.g., name, title, organizational unit, business email and phone), plus additional information necessary to verify the individual's authorization to receive classified information or controlled unclassified information (e.g., security clearance, citizenship). This information is required by the DIB CS/IA program office to manage the program and interact with the companies through routine emails, phone calls, and participation in periodic classified meetings. A DIB company that is not yet participating in the Program may also provide POC information to the DIB CS/IA Program office in order to discuss Program application procedures or related information regarding the Program.

In addition to the designation of a limited number of primary POCs for the DIB company's overall participation in the DIB CS/IA Program, additional POC information may be provided in the individual incident reports submitted by the company. In most cases, the DIB companies report incidents using a DIB CS/IA Program standardized Incident Collection Form (ICF), which is submitted as the initial incident report to the DoD-DIB Collaborative Information Sharing Environment (DCISE) at DC3. The ICF includes the basic POC information (e.g., name, organizational unit, business email and phone) for the DIB company representative who is submitting the initial report. The ICF also allows the reporting company to provide the same basic POC information for other company personnel that are knowledgeable about, or otherwise relevant for, the reported incident (e.g., POCs for incident response, technical issues, or the affected business unit). In some cases, a company may elect to report the incident without using the ICF; and companies may report incidents through a variety of communications channels, including email, fax, or by phone, if necessary.

Collecting this type of POC information is the only element of this information sharing activity in which the DIB CS/IA program intentionally collects PII; however, there are other portions of the information sharing activities that present the potential for the DIB companies to provide DoD with PII that is incidental to, or embedded within, other cyber security information being shared—resulting in an inadvertent collection of PII.

2. Cyber Incident Response and Analysis:

Although it is not typical or expected, it is nevertheless possible that a DIB company may voluntarily submit PII to DoD in connection with the initial cyber incident reporting or response activities, or during follow-up digital forensics or damage assessment activities. Accordingly, the Program is designed to provide appropriate handling and safeguards in the event that PII is (inadvertently) collected in these circumstances.

For example, when providing the initial incident report on the ICF, the DIB company provides a description of the cyber incident, including technical and contextual details regarding any or all relevant aspects of the incident. In some cases, the DIB company may determine that PII, or what appears to be PII, is relevant in describing the event (e.g., an individual's name and email address that may be spoofed in connection with an email phishing attempt or an email used as the delivery mechanism for malware). The ICF allows the company to describe the incident in two levels of detail and sensitivity: (i) a fully detailed version that may contain attribution or other sensitive information (e.g., PII) that the company is providing for internal DCISE use; and (ii) an alternative description that provides only such information that the company is authorizing to be released outside the DCISE for cyber security purposes (e.g., as part of an automated "alert" process that immediately forwards only this company pre-approved information to all participating DIB companies). Subsequently, the DCISE also follows up with the DIB company to confirm the nature and extent of information that the DIB company authorizes for release outside the DCISE for cyber security purposes (except in cases when the company has indicated that it does not desire this additional pre-release review).

In addition, the DoD and DIB companies have recognized that, in some cases, after the initial incident report and preliminary investigation, a more complete analysis of the event may be necessary. Accordingly, on a voluntary basis, DIB companies may share additional information about potentially compromised information systems with the DoD for this purpose. This information may include PII or other sensitive information that the DIB company determines is relevant for the analysis, but the DIB companies may elect to limit the nature and extent of any sensitive information to be shared, due to legal, contractual, or other restrictions (e.g., the DIB company determines that it is not authorized to share certain PII or third-party proprietary information with the DoD, even if it would be relevant to the cyber event analysis).

Similarly, as part of the follow-up for each reported incident, the DIB company reviews the potentially compromised systems or networks and reports to DoD regarding the presence of files or information associated with DoD programs, systems, or military applications. When the reported cyber intrusion affects systems containing such DoD information, the DIB companies will preserve and share with DoD the unclassified files on threat-accessed systems that pertain to Government programs, unless there are legal or contractual reasons that preclude sharing (e.g., the images may contain PII or third-party proprietary information that are subject to nondisclosure prohibitions). The DoD's Damage Assessment Management Office (DAMO), an organizational element of the Under Secretary of Defense for Acquisition, Technology and Logistics, reviews the available information to determine whether a more complete damage assessment is warranted.

The short-term DIB Cyber Pilot also utilizes the incident reporting procedures already established for the DIB

CS/IA Program, although it is anticipated that the DIB companies will typically be reporting less detailed information regarding incidents detected by the DIB companies' commercial service providers (CSPs), given the limited proof-of-concept nature of the Pilot and the fact that it was the CSP, rather than the DIB company, that detected the event. DIB companies participating in the voluntary 90-day proof-of-concept pilot notify DC3 of an incident when they determine an incident occurred based on an alert from their commercial service provider. Consistent with the reporting procedures for the existing DIB CS/IA Program, the DIB companies participating in the Pilot will include PII in their incident reporting and follow-up analysis only if the DIB company determines that the PII is relevant and material to the understanding of the technical attributes of the incident, and that there are no legal, contractual, or other restrictions on sharing that PII with the USG. There is no incident reporting from the CSP to the USG under the Pilot, although that CSPs may voluntarily provide the USG with end-of-pilot lessons learned or other general feedback regarding the Pilot activities (e.g., technical or operational issues and solutions arising during the exercise)—none of which will include PII.

These information sharing mechanisms are intended to enhance a participating DIB company's ability to detect and defend against cyber intrusions and other malicious activity occurring on their networks, in order to better protect Defense information. In doing so, the DIB CS/IA Program has developed uniform procedures and safeguards (e.g., set forth in the standardized FAs) designed to ensure that the DIB companies share information with DoD only if it is relevant to the forensics or damage assessment analysis, and only after the DIB company verifies that it is authorized to share the information with the DoD for these purposes.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

There are minimal risks associated with the PII collected in connection with the DoD-DIB cyber security information sharing activities under the DIB CS/IA Program. The Program's information sharing activities implement administrative, technical, and electronic protections to ensure compliance with all applicable DoD policies and procedures regarding the collection and handling of PII and other sensitive information, including but not limited to the following:

- DoDD 5400.11, "DoD Privacy Program", May 8, 2007
- DoD 5400.11-R, "Department of Defense Privacy Program", May 14, 2007
- DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- DoD CIO memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)", August 18, 2006
- DA&M memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", June 05, 2009
- DoDI 8500.02, "Information Assurance Implementation," February 6, 2003
- DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- DoDI 5200.1, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008 (Revised June 13, 2011)
- DoD 5200.1-R, "Information Security Program," January 14, 1997
- DoDI 5015.2, "DoD Records Management Program," March 6, 2000

(These references are publicly available, e.g., at <http://www.dtic.mil/whs/directives/> or http://dpclo.defense.gov/privacy/About_The_Office/policy_guidance.html.)

The Program is also structured around several key elements that are designed to ensure that risks are effectively addressed to safeguard privacy:

- All PII received by the DoD is provided voluntarily by authorized DIB company representatives, subject to mutually agreed upon restrictions (e.g., in the FA);
- The nature of the PII being intentionally collected is limited to ordinary business contact information for DIB company personnel;
- PII is inadvertently collected only if submitted by a DIB company that has determined that the PII is relevant to cyber incident response and analysis activities, and that the PII is authorized to be shared with the DoD for these purposes;
- Once collected, access and use of PII is limited to authorized personnel that need the information for cyber security or other lawful purposes;
- All DIB CS/IA Program and supporting personnel receiving access to the collected PII are required to

undergo training and are subject to appropriate nondisclosure restrictions; and

- The PII is maintained for only so long as necessary for DIB CS/IA Program activities, and is managed and disposed of in accordance with applicable records management requirements.

Additional details regarding these risk mitigations and safeguards are discussed below.

*** Collection of Information:**

The DIB CS/IA information sharing activities covered by this PIA are focused on sharing cyber security related information, and thus the Program seeks to minimize the collection and management of PII except as necessary to support the program. The operational implementation of this sharing arrangement involves sharing and managing PII in two supporting or incidental ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) for cyber incident response and analysis purposes, although it is not typical or expected, there exists the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for the cyber security analysis.

As discussed previously, the DIB CS/IA Program intentionally collects PII regarding DIB company POCs only for routine program administration and management purposes. This PII does not involve any particularly sensitive personal information – it is limited to the individual's typical contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone), including other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program. Any other PII collected under the Program is inadvertently collected, in that it is provided to DoD by a participating DIB company based on that company's determination that the PII is relevant to the incident response and analysis, and that there are no legal, contractual, or other restrictions on sharing that PII with the USG for these purposes.

Additional details on the nature and circumstances of PII collection for these purposes are discussed in more detail in Section 2.g.(1) above.

*** Use and Management of Collected Information:**

The DIB company POC information may not be a particularly sensitive type of PII, it is nevertheless tightly controlled within the DIB CS/IA Program – in the same manner and for the similar purposes, that the Program controls DIB company "attribution information" (i.e., information that identifies a company or its programs, whether directly or indirectly, by the grouping of information that can be traced back to that company). Although the name of a DIB company or its programs, or the basic contact information for the company's POCs, might not ordinarily be considered particularly sensitive, the association of that company or its specific POCs with particular cyber security activities, or with particular cyber security incidents, may be treated as sensitive. Accordingly, the DIB CS/IA Program restricts access to such PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. For example, all USG personnel and contractors directly supporting the DIB CS/IA Program (including the Program Office, DC3, and DAMO personnel or contractors) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

Regarding information provided for incident response and analysis, DC3 will maintain, control, and dispose of all media provided by DIB companies in accordance with established DoD policies and procedures for the handling and safeguarding of PII and other sensitive information, and DC3 also implements specialized handling procedures to maintain its accreditation as a digital and multimedia forensics laboratory. DC3 personnel determine that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA activities before such data is further processed or retained. Information deemed unnecessary for subsequent analysis is purged immediately. In accordance with NARA regulation and 36 CFR §1220-1239, program records are retained for a minimum of three (3) years, and tracking/ticketing system records are retained for a minimum of two (2) years. The media are protected using procedural controls that are the same as, or similar to, those DC3 uses to handle evidence that it processes as part of criminal investigations. Access to electronic media/files that may have PII or other sensitive information, is strictly controlled and limited to those participating in

formal DIB cyber intrusion analyses or damage assessments. The electronic media/files are maintained by the digital and multimedia forensics laboratory—the files and media do not leave DC3, physically or electronically.

The Program's information sharing procedures are designed to ensure that PII and other sensitive information is shared and processed by DoD only after the submitting DIB Company has determined that the information is relevant to cyber intrusion incidents or follow-on forensics or cyber intrusion damage assessment analysis, and that the information has been lawfully collected and is authorized for sharing with the DoD. When sharing electronic images or files with the DoD for forensics or damage assessment activities, the DIB companies will identify the types of sensitive information (e.g., PII, proprietary, export controlled) that may be contained in the shared files. In addition, when the DoD is performing its analysis on the files, it may discover PII (or other sensitive information) that had not been identified by the DIB company when the information was submitted. If this occurs, all investigative work involving that PII ceases, the DIB company is notified that the PII (or sensitive information) was discovered, and the DIB company provides guidance as to the disposition of that information.

*** Dissemination of Information:**

For cyber security purposes, DC3, based on analysis of specific cyber threats, releases threat information containing indicators developed from numerous data sources (e.g., government, DIB companies, open source). DC3 will disseminate cyber threat information that may contain PII only after the information has been reviewed and approved for release, including coordination with the source of the PII. For example, release of cyber threat indicators derived from information provided by government sources are coordinated with key government stakeholders, such as USCYBERCOM and NSA. Similarly, indicators derived from information contained in DIB company incident reporting will be disseminated only after coordination with the reporting company (regardless of whether the indicator contains PII).

When cyber threat information is shared with DIB companies under the Program, the DIB company is required to ensure that unclassified threat information is shared with authorized company personnel that have a need-to-know the information for the company's internal cyber security activities. Typically, the unclassified portion of threat information products may be shared with Company network security personnel. The DIB companies are prohibited from sharing the threat information products outside of the company's U. S. based information systems without specific written Government authorization.

The Director, DC3 (DDC3), or designee, must approve any dissemination of information by DC3 for law enforcement/counter intelligence purposes to support an investigation and prosecution of any individual or organization when the information appears to indicate activities that may violate laws, including those attempting to infiltrate and compromise information on a Company information system. Such dissemination must comply with the Privacy Act and other applicable statutes, regulations, and DoD policies, including those references listed above (section 2.g.(2)).

*** Records Management and Retention of Information:**

The DIB company POC information provided to support the DIB CS/IA administration and management process is maintained only so long as the designated POC(s) continue to represent the participating company for the Program. When the DIB CS/IA program office is notified that a DIB company POC is being replaced, the POC information databases are updated and outdated PII is archived in accordance with records management requirements.

Inadvertently collected PII that may be submitted by DIB companies in connection with incident reporting and response is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA activities before such data is further processed or retained. Information deemed unnecessary for subsequent analysis is purged from DC3 systems. Information determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes). The time it takes to complete a cyber intrusion forensics analysis and damage assessment will vary. Some of the assessments will be more complex and require more time than others.

In all cases, the management and disposal of this information will comply with all applicable DoD records management procedures and requirements, and records disposition schedules. In accordance with NARA regulation and 36 CFR §1220-1239, program records are retained for a minimum of three (3) years, and

tracking/ticketing system records are retained for a minimum of two (2) years.

*** Compliance and Oversight Mechanisms:**

The DIB CS/IA baseline program and opt-in pilot have been subject to review by and consultation with the Defense Privacy and Civil Liberties Office (DPCLO). DC3 and DPCLO will work with existing DoD inspection agencies to ensure that adequate privacy and civil liberties oversight mechanisms exist. All DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems (see DoDI 8010.01). In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory.

*** Additional Considerations:** Will the networks that store or process the PII be monitored? How would participating entities know that their networks are subject to monitoring?

None of these DIB CS/IA activities involve any DoD or USG personnel performing any monitoring of DIB company or other private networks. The DIB companies are responsible for the conduct of any monitoring of their own networks, and for ensuring that there are no legal, contractual, or other restrictions on sharing of PII or any other sensitive information with the DoD. The only PII received by DoD under these activities is PII that is provided directly to DoD by authorized DIB company personnel.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)?
Indicate all that apply.

Within the DoD Component.

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to those authorized personnel that have a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to appropriate nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is maintained at DC3 with strict accountability and need-to-know on those DoD and support contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

Other DoD Components.

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to other authorized DoD Component personnel that are authorized to receive the information under the FA, based on a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to appropriate nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is maintained at DC3 with strict accountability and need-to-know on those DoD and support contractor personnel having access to the files. All other DoD Component personnel and contractors directly supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements

requiring training and providing strict guidelines on the handling and protecting of that information.

Other Federal Agencies.

Specify.

PII is shared with other federal agency authorized personnel only for cybersecurity purposes (as authorized by the DIB companies under the FA, and following the incident response and follow-on analysis coordination procedures previously discussed), and in support of authorized LE/CI activities (or other lawful purposes). Only such PII as authorized by the company will be released outside of the DoD.

State and Local Agencies.

Specify.

[Empty text box]

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

The DIB CS/IA Program restricts access to PII and attribution information only to those authorized support contractor personnel that have a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to strict nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is maintained at DC3 with strict accountability and need-to-know on those USG and DoD support contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information. PII that is derived from DIB company submitted information and is included in DC3 threat products will be shared with other DIB companies participating in the DIB CS/IA Program, as authorized under the FA, and following the incident response and follow-on analysis coordination procedures previously discussed.

Other (e.g., commercial providers, colleges).

Specify.

In any other case, DoD would not share the PII except after obtaining the appropriate permission (e.g., from the DIB company or the individual identified by the PII).

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she can object to the collection of PII at that time.

(2) If "No," state the reason why individuals cannot object.

DIB company POC information may also be intentionally collected from a DIB company representative that is

providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to object at this point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

- Yes No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she is provided the opportunity to consent or not consent to specific uses of PII when they are presented with a Privacy Act Statement.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DIB company POC information may also be intentionally collected from a DIB company representative that is providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to consent or withhold consent for specific uses at the point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- Privacy Act Statement Privacy Advisory
 Other None

Describe each applicable format.

Privacy Act Statement to include the authorities to collect the information; the purpose or purposes for which the information is to be used; the routine uses that will be made of the information; whether providing the information is voluntary or mandatory and the effects on the individual if he or she chooses not to provide the requested information.

DoD Office of General Counsel

DIB Pilot Legal Construct & Framework Agreements



07 July 2010

(b) (6)

Associate General Counsel



Overview

- **Overview of the Legal Construct**
- **The Partnering Triangle**
- **Framework Agreement Elements That Are Not Affected**
- **Sharing the Enhanced Threat Information Products**
- **Event Reporting and Sharing of Information**
- **DIB Partner Informed Consent**
- **Questions?**



The Legal Construct

Voluntary

Informed

Consent



The Legal Construct

- **Basic Authority: DoD Information Assurance**
 - DIB Cyber Security/Information Assurance Program
 - Critical Infrastructure Protection Activities

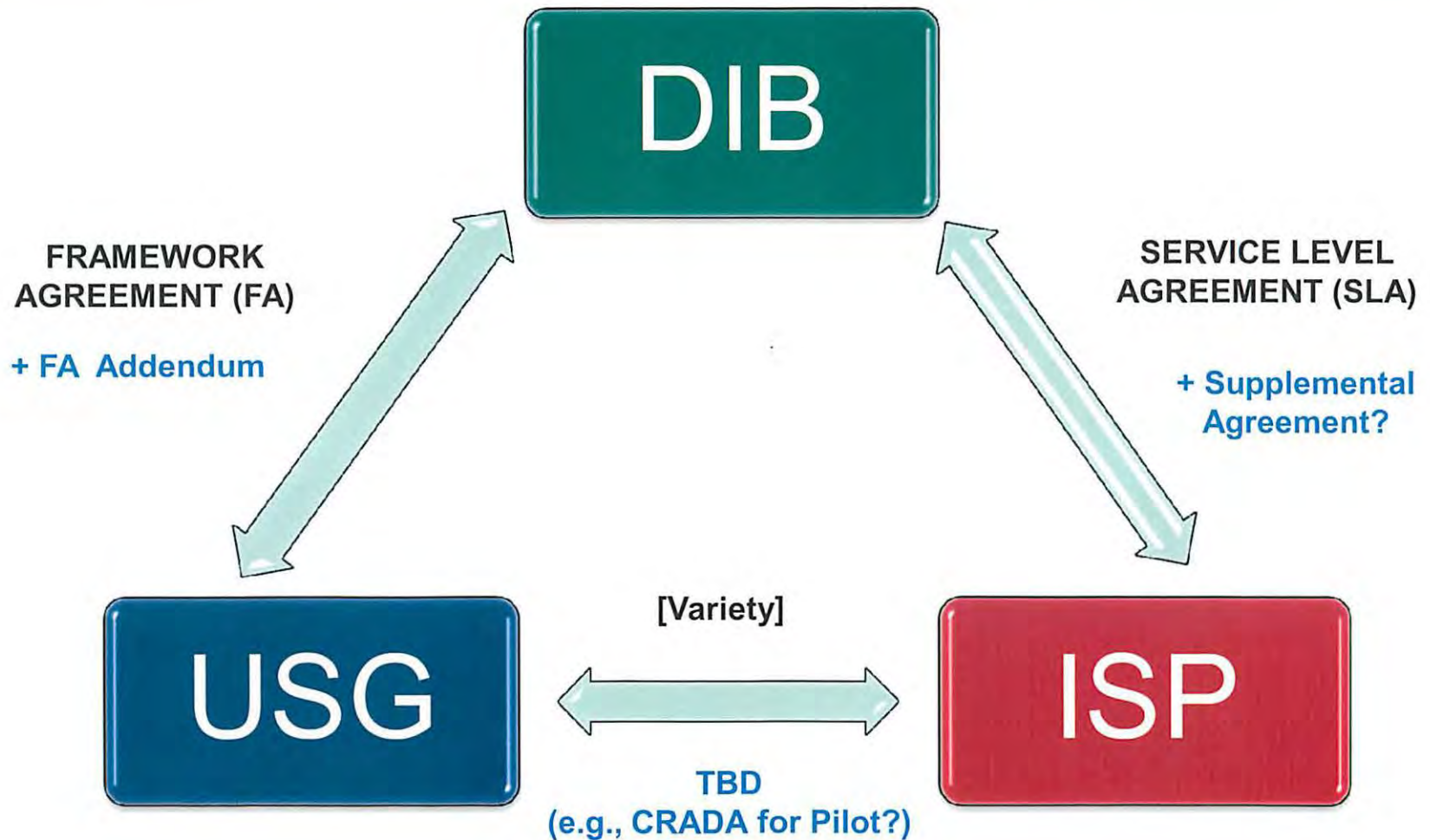
 - **Leverage existing relationships, mechanisms**
 - Add new benefits – supplementing the current state

 - **Avoid legal obstacles to detecting, reacting, sharing information regarding malicious cyber events**
 - Constitutional: 4th Amendment
 - Statutory: Wiretap Act, Stored Communications Act, Computer Fraud & Abuse Act, Pen/Trap & Trace
 - Contractual: effect on existing obligations, restrictions

 - **Voluntary, Informed, Consenting, Partnership – "Opt In"**
-



The Partnering Triangle





FA Elements NOT Affected

- **Government Threat Information Products** currently provided . . . and being improved continuously

- **DIB Partner Reporting** of Tier-1 or -2 cyber intrusion events

- **Follow-up → Detailed Forensics & Damage Assessment**

- **Protection for Shared Information**
 - E.g., Attribution Information, FOUO/Classified threat info



The Enhanced Threat Information Products

- **Additional, classified threat information products**
 - Example: TS/SCI signatures, actionable info, countermeasures
 - Not available from other sources
 - Not available under the current FA sharing mechanisms
 - For the Pilot: limited to two specific types of countermeasures

- **Goal: minimize deployment profile/exposure** – in reaching the maximum number of DIB Partners

- **Products provided directly to DIB Partner ISP(s)**
 - Deployed in a secure, USG-approved
 - Applied to consenting DIB Partner internet traffic
 - Enhancement to existing ISP services



Reporting & Sharing of Cyber Event Information

- **Enhanced Products** – enable automated (configurable) detection, response, and reporting
 - Reacts **ONLY** to known, malicious events/criteria
 - Capability to engage and defeat the attempted malicious act

- **Reporting available to--**
 - DIB Partner
 - ISP
 - USG

- **Types of Reporting**
 - Real-time vs. periodic/aggregated
 - Detailed vs. aggregated or anonymized



DIB Partner Consent

- **Actual Consent is the CORE approach to avoid legal barriers to—**
 - Applying the countermeasures
 - Sharing the information regarding malicious events

 - **DIB Partner "Entity" Consent**
 - Addendum to the FA with DoD – outlines the new process
 - Agreement with the ISP regarding effect on services

 - **DIB Partner – "User's" Consent**
 - Example: logon banners, user agreements, training
 - DIB Partner certifies adequate procedures in place. . .
-



Notional FA Addendum Structure

- **Purpose:** Scope/purpose of the opt-in pilot
- **Definitions:** "Enhanced Threat Information Products" (classified appendix, if needed)
- **Sharing ETIPs:** Directly with designated ISP
- **Reporting:** Define nature, type, timing to DIB, ISP, USG
- **Express Consent:** for DIB entity, and ensuring DIB network users



Questions?

Richard M. Gray

**Associate General Counsel
Department of Defense
Office of the General Counsel**

Direct: [REDACTED] (b) (6)

NIPR: [REDACTED] (b) (6)

SIPR: [REDACTED] (b) (6)

JWICS: [REDACTED] (b) (6)





BACKUP SLIDES

UNCLASSIFIED // FOR OFFICIAL USE ONLY



Selected Legal References

- Information Assurance
 - 10 USC 2224, Defense IA Program; 44 USC 3541 et seq., FISMA
 - Critical Infrastructure Protection
 - HSPD-7, Critical Infrastructure Protection
 - Comprehensive National Cybersecurity Initiative
 - NSPD-54/HSPD-23
 - Crimes Against Computers or Communications Systems
 - 18 U.S.C. § 1030, Fraud and Related Activity in Connection with Computers
 - 18 U.S.C. § 2510 et seq, Wire and Electronic Communications Interception and Interception of Oral Communications
 - 18 U.S.C. § 2701 et seq, Stored Wire and Electronic Communications and Transactional Records Access
 - 18 U.S.C. § 3121 et seq, Recording of Dialing, Routing, Addressing, and Signaling Information
-

DoD Office of General Counsel

Discussion Points: Key Elements for Notice and Consent Banners



Defense Industrial Base Cybersecurity
Exploratory Initiative Meetings
December 2-3 2010

(b) (6)

Associate General Counsel
Department of Defense
Office of the General Counsel

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



Disclaimer

- This briefing is being provided for informational and discussion purposes only and does not constitute legal advice, nor create any attorney-client relationship. The Department of Defense Office of General Counsel is not acting as your attorney. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this briefing. We likewise do not warrant the legal effect of these materials.
- The law changes very rapidly and, accordingly, we do not guarantee the accuracy or currency of this information is accurate and up to date. The law differs from jurisdiction to jurisdiction, and is subject to interpretation of courts located in each state or county. Legal advice must be tailored to the specific circumstances of each case and the tools and information provided to you may not be an appropriate fit in your case.
- The opinions expressed in the presentation of these materials are those of the individual contributors to or presenters of these materials and do not necessarily represent, and should not be attributed to, the Department of Defense or the United States Government.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



Overview

8 Key Elements for Notice and Consent Banners

1. It expressly covers *monitoring* of data and communications *in transit* rather than just accessing data *at rest*.
2. It provides that information transiting or stored on the system may be *disclosed* for any purpose, including to the Government.
3. It states that monitoring will be *for any purpose*.
4. It states that monitoring may be done by the Company/Agency or *any person or entity authorized by Company/Agency*.
5. It explains to users that they have "*no [reasonable] expectation of privacy*" regarding communications or data transiting or stored on the system.
6. It clarifies that this consent covers *personal use* of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.
7. It is *definitive* about the fact of monitoring, rather than conditional or speculative.
8. It expressly *obtains consent* from the user and does not merely provide notification.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

3



1. It expressly covers *monitoring* of data and communications *in transit* rather than just accessing data *at rest*.

Notes:

- Use the terms "monitoring" and/or "intercept."
- This requirement is driven by the Wiretap Act and Stored Communications Act.

Examples:

- "You consent to the unrestricted monitoring, interception...of all communications and data transiting or stored on this system...."
- "You consent, without restriction, to all communications and data transiting or stored on this system being monitored, intercepted..."

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

4