

From: [Andrew, Emily](#)
To: [Falkenstein, Cindy](#)
Subject: RE: DoD to Expand DIB Cyber program
Date: Monday, August 22, 2011 7:48:55 AM

Cindy – can you add: (b) (5) for today?

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

Emily,

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

(b) (5)

(b) (5)

.. seems like exactly the same thing...

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

18 August 2011

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

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

Lynn [told](#) the conference that the pilot program had already stopped hundreds of attempted network intrusions.

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

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

The *Washington Post* identified a number of the companies participating in the pilot program, including Lockheed Martin, CSC, SAIC, Northrop Grumman, as well as AT&T, Verizon, and CenturyLink.

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

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

John W. Kropf
Deputy Chief Privacy Officer
Privacy Office
U.S. Department of Homeland Security
245 Murray Lane, SW, Mail Stop 0655
Washington, DC 20528-0655
Telephone: (b) (6)
Fax: (b) (6)
(b) (6)

Andrew, Emily

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

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

By Chris Strohm

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

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

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

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

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

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

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

No Personal Communications

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

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

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

For Related News and Information:

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

--Editors: Michael Shepard, Romaine Bostick


DIB PILOT CALL WITH BLOOMBERG

Talkers:

The Administration decided recently to temporarily extend the Defense Industrial Base (DIB) Cybersecurity Pilot during U.S. Government deliberations. During the extension, DHS will take responsibility for managing the government relationship with Commercial Service Providers participating in the Pilot. DHS will be the principal interface between the government and the participating commercial service providers. DOD will continue to be the interface with the participating DIB companies.

DHS leads the government-wide effort to protect critical infrastructure within the United States, including critical information infrastructure.

(b) (5)



(b) (6)

From: Denning, John
Sent: Wednesday, July 07, 2010 6:02 PM
To: Brown, Michael A.; Schaffer, Gregory
Cc: Mesterhazy, Paul; (b) (6) (b) (6) Jones, Jeremiah; (b) (6)
Subject: ESF Connection

(b) (5)

HR 5136/S 3454 Sec. 215 (b) (5)

Demonstration and pilot projects on cybersecurity (sec. 215)

The committee recommends a provision that would require the Secretary of Defense, in support of and in coordination with the Secretary of Homeland Security, to develop and conduct pilot demonstrations to determine the potential contribution of commercial technology and capabilities to the defense of government and defense industrial base cyber networks and systems, and various means by which the government can acquire or apply those commercial technologies and capabilities.

The committee strongly supports the potential piloting projects recently developed within the executive branch, and recommends authorization of \$30.0 million to execute the pilots described in this section. The committee is heartened that the administration is finally recognizing the enormous potential role for the private sector in cybersecurity. The funding would be authorized in line 196, Research, Development, Test, and Evaluation, Defense-wide, PE 32019K.

The committee is persuaded that the major telecommunications and Internet Service Providers, collectively, have unparalleled visibility into global networks which would enable them to detect cyber intrusions and attacks as they are forming and transiting towards their targets. These companies also already possess potent tools and techniques for countering these attacks in order to defend their own infrastructure and the networks and applications of their customers. However, while each of the major companies possesses impressive visibility, it is only by combining their collective network visibility that a comprehensive, global warning and assessment capability can be achieved. Furthermore, while these companies already share information about threats and problems, they do so on an ad hoc and non-real-time basis. An integrated attack warning and response capability requires an engineered, real-time exchange and consolidation of threat information and response capabilities.

The committee believes that it is essential for the administration to determine how a commercial consortium could be formed, what the government's role would be in establishing and managing such a consortium, and how the government could and should participate. The committee is aware that there are significant legal and policy issues that would need to be carefully worked through, including possible anti-trust concerns and legal restrictions on the sharing of the content of communications with the government, even if that content is malicious software. The committee's intent is that the administration proceed as far as it can as soon as it can, on a pilot basis, but completely within the confines of existing policy and legal constraints. The

administration should not wait to begin those elements of this pilot that can be pursued right away until it has sorted out and resolved all the issues associated with a fully operational commercial consortium that is integrated into government security operations centers.

The committee stresses that this commercial consortium pilot depends on sponsorship from the Department of Homeland Security (DHS), and that the DOD role would be to support DHS.

The committee is also very interested in the potential for commercially outsourced, managed security services to rapidly increase the security of key elements of the Defense Industrial Base. If this pilot is successful, it could provide a model for defending other privately owned critical infrastructure, as well as federal departments and agencies, consistent with the Managed Trusted Internet Protocol Services program executed by the General Services Administration (GSA), which now includes managed security services under the Networx contract vehicle.

This model also could be easily extended to encompass outsourcing of network services and computing, including cloud computing. The committee believes that there is evidence to support the contention that such comprehensive outsourcing would provide better service and far better security, at equal or even reduced cost. The committee notes that GSA achieved precisely these results through its own cloud outsourcing program.

The committee hopes that these two pilots could demonstrate that there are means to dramatically improve the Nation's cybersecurity capabilities rapidly, affordably, and without taxing the limited abilities of DHS and other federal organizations to manage complex systems acquisitions. The models demonstrated through these pilots also could complement, and be integrated with, the Einstein 3 program, and existing defense-in-depth cybersecurity capabilities within the Department of Defense, the Department of State, the Department of Justice, and elsewhere.

A third pilot would involve creating a commercial construct and processes that would permit DOD to rapidly acquire operational or technical cyber capabilities from the private sector, to incentivize commercial investments in technology and capabilities, and to facilitate the transition of these capabilities into both government programs and commercial markets. A major goal would be to achieve agility in exploiting innovations and closing vulnerabilities. The committee expects that this pilot would contribute to the cyber acquisition strategy that would be required by sec. 933 of this Act.

The provision would require DOD to conduct a fourth pilot whose purpose would be to develop a process to enable the evaluation and comparison of commercial cyber security products and services across a common set of standards and a common taxonomy. The committee intends that the Department exploit the work of the private sector's development of the Consensus Audit Guidelines and the security controls developed by the National Institute of Standards and Technology. These guidelines and controls are based on the most significant attack patterns, and could form a framework for organizing and integrating commercial products and services.

The committee understands that these pilots will take some time to initiate and complete, but expects the Department to be aggressive, in keeping with the Department's own declared anxiety about the rising cybersecurity threat and the need for forceful corrective action.

Office of Cybersecurity and Communications

Department of Homeland Security

Desk: (b) (6)

Secondary: (b) (6)

Back-up: (b) (6)

Pager: (b) (6)

Web: www.dhs.gov/cyber

(b) (6)

From: Brown, Michael A.
Sent: Thursday, August 19, 2010 6:22 AM
To: Stempfley, Roberta; Dean, Nicole M
Subject: Fw: Defense Supp Dates

(b) (5)

From: Brown, Michael A.
To: Reitingner, Philip; Durkovich, Caitlin; Beers, Rand
Cc: Schaffer, Gregory; McConnell, Bruce; Dorville, Kristina
Sent: Thu Aug 19 06:15:11 2010
Subject: Re: Defense Supp Dates

Sir,

Roger.

Vr,
Mike

From: Reitingner, Philip
To: Brown, Michael A.; Durkovich, Caitlin; Beers, Rand
Cc: Schaffer, Gregory; McConnell, Bruce; Dorville, Kristina
Sent: Thu Aug 19 06:08:15 2010
Subject: RE: Defense Supp Dates

Pls set up a briefing for me so we can discuss and I can provide input or direction. Thank you.

From: Brown, Michael A.
Sent: Thursday, August 19, 2010 5:58 AM
To: Reitingner, Philip; Durkovich, Caitlin; Beers, Rand
Cc: Schaffer, Gregory; McConnell, Bruce; Dorville, Kristina
Subject: Re: Defense Supp Dates

Sir,

(b) (5)

Vr,
Mike

From: Reitingner, Philip
To: Durkovich, Caitlin; Beers, Rand
Cc: Brown, Michael A.; Schaffer, Gregory; McConnell, Bruce; Dorville, Kristina
Sent: Thu Aug 19 05:50:32 2010
Subject: RE: Defense Supp Dates

Thank you, Caitlin.

(b) (5)

phil

From: Durkovich, Caitlin
Sent: Thursday, August 19, 2010 12:12 AM
To: Reiting, Philip; Beers, Rand
Cc: Brown, Michael A.; Schaffer, Gregory; McConnell, Bruce
Subject: Defense Supp Dates

Phil -

Per our conversation this afternoon,

(b) (5)

Deadlines of note:

- NSC, in coordination with the Secretary of DHS, will provide a report to the Committees on Appropriations and other appropriate committees NLT November 15, 2010, on the details of that plan, the exercise of the plan conducted to date, the lessons learned from those exercises, and any resulting recommendations for changes or further actions to be taken.
- DoD and DHS, in conjunction with other relevant Federal agencies, are directed to jointly produce an execution plan to undertake cybersecurity pilot programs, to be submitted to the Committees on Appropriations no later than 90 days (approx Oct 29) after the date of enactment of this act.
- All pilots shall be able to be implemented in no more than 1 year.

Caitlin

EXECUTIVE OFFICE OF THE PRESIDENT AND FUNDS APPROPRIATED TO THE PRESIDENT

NATIONAL SECURITY COUNCIL

CYBERSECURITY INCIDENT RESPONSE

It is essential that the United States Government has an effective organization for rapidly providing a coordinated response to a cyber attack. The White House released its cyberspace policy review on May 29, 2009, which requires the development of a cybersecurity incident plan, including the contributions of the private sector; and a process between the Government and the private sector to assist in preventing, detecting, and responding to cyber incidents. While the Committee is encouraged that efforts are underway to develop a National Cyber Incident Plan, and to exercise that plan, 12 months have passed and Congress has not received recommendations on how to meet the requirement contained in the May 29 policy review. The Committee

directs the National Security Council, in coordination with the Secretary of Homeland Security to provide a report to the Committees on Appropriations and other appropriate committees of Congress no later than November 15, 2010, on the details of that plan, the exercise of the plan conducted to date, the lessons learned from those exercises, and any resulting recommendations for changes or further actions to be taken.

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

INFRASTRUCTURE PROTECTION AND INFORMATION SECURITY

CYBERSECURITY PILOTS

The cybersecurity threat continues to evolve and the Nation's responses against this threat must be agile. In order to keep pace, Federal agencies with major responsibilities in this area should ensure cutting-edge solutions are made available for Government use as soon as possible. A clear plan to test and evaluate evolving solutions through pilot programs is a prudent method to ensure the best investments are made. Therefore, the Department of Defense and the Department of Homeland Security, in conjunction with other relevant Federal agencies, are directed to jointly produce an execution plan to undertake cybersecurity pilot programs, to be submitted to the Committees on Appropriations no later than 90 days after the date of enactment of this act. The pilot programs shall illustrate how innovative commercial technologies can be quickly identified and effectively applied to national cybersecurity requirements and to explore how these innovative technologies can be deployed across Government agencies and key elements of the private sector consistent with an executable operational concept.

Each pilot, to the extent possible, should maximize the work of the other pilots while also recognizing the authorities and leadership of the respective Federal agency taking the lead for the pilot. All pilots shall avoid unnecessarily disrupting the execution of ongoing programs and should inform decisions on deployment of operational capabilities; reflect a feasible legal and operational construct; have some track record of success to reduce risk; and be able to be implemented in no more than 1 year. This effort shall not conflict with, but instead contribute to, the President's Cyberspace Policy Review and the Comprehensive National Cybersecurity Initiative.

(b) (6)

From: (b) (6)
Sent: Thursday, July 08, 2010 5:51 AM
To: Denning, John; Brown, Michael A.; Schaffer, Gregory
Cc: Mesterhazy, Paul; (b) (6) (b) (6) Jones, Jeremiah
Subject: RE: ESF Connection

(b) (5)

(b) (6)

Special Assistant to the Deputy Assistant Secretary
 Cyber Security and Communications
 Department of Homeland Security

(b) (6)

(b) (6)

From: Denning, John
Sent: Wednesday, July 07, 2010 6:02 PM
To: Brown, Michael A.; Schaffer, Gregory
Cc: Mesterhazy, Paul; (b) (6) (b) (6) Jones, Jeremiah; (b) (6)
Subject: ESF Connection

(b) (5)

HR 5136/S 3454 Sec. 215

(b) (5)

Demonstration and pilot projects on cybersecurity (sec. 215)

The committee recommends a provision that would require the Secretary of Defense, in support of and in coordination with the Secretary of Homeland Security, to develop and conduct pilot demonstrations to determine the potential contribution of commercial technology and capabilities to the defense of government and defense industrial base cyber networks and systems, and various means by which the government can acquire or apply those commercial technologies and capabilities.

The committee strongly supports the potential piloting projects recently developed within the executive branch, and recommends authorization of \$30.0 million to execute the pilots described in this section. The committee is heartened that the administration is finally recognizing the enormous potential role for the private sector in cybersecurity. The funding would be authorized in line 196, Research, Development, Test, and Evaluation, Defense-wide, PE 32019K.

The committee is persuaded that the major telecommunications and Internet Service Providers, collectively, have unparalleled visibility into global networks which would enable them to detect cyber intrusions and attacks as they are forming and transiting towards their targets. These

companies also already possess potent tools and techniques for countering these attacks in order to defend their own infrastructure and the networks and applications of their customers. However, while each of the major companies possesses impressive visibility, it is only by combining their collective network visibility that a comprehensive, global warning and assessment capability can be achieved. Furthermore, while these companies already share information about threats and problems, they do so on an ad hoc and non-real-time basis. An integrated attack warning and response capability requires an engineered, real-time exchange and consolidation of threat information and response capabilities.

The committee believes that it is essential for the administration to determine how a commercial consortium could be formed, what the government's role would be in establishing and managing such a consortium, and how the government could and should participate. The committee is aware that there are significant legal and policy issues that would need to be carefully worked through, including possible anti-trust concerns and legal restrictions on the sharing of the content of communications with the government, even if that content is malicious software. The committee's intent is that the administration proceed as far as it can as soon as it can, on a pilot basis, but completely within the confines of existing policy and legal constraints. The administration should not wait to begin those elements of this pilot that can be pursued right away until it has sorted out and resolved all the issues associated with a fully operational commercial consortium that is integrated into government security operations centers.

The committee stresses that this commercial consortium pilot depends on sponsorship from the Department of Homeland Security (DHS), and that the DOD role would be to support DHS.

The committee is also very interested in the potential for commercially outsourced, managed security services to rapidly increase the security of key elements of the Defense Industrial Base. If this pilot is successful, it could provide a model for defending other privately owned critical infrastructure, as well as federal departments and agencies, consistent with the Managed Trusted Internet Protocol Services program executed by the General Services Administration (GSA), which now includes managed security services under the Networx contract vehicle.

This model also could be easily extended to encompass outsourcing of network services and computing, including cloud computing. The committee believes that there is evidence to support the contention that such comprehensive outsourcing would provide better service and far better security, at equal or even reduced cost. The committee notes that GSA achieved precisely these results through its own cloud outsourcing program.

The committee hopes that these two pilots could demonstrate that there are means to dramatically improve the Nation's cybersecurity capabilities rapidly, affordably, and without taxing the limited abilities of DHS and other federal organizations to manage complex systems acquisitions. The models demonstrated through these pilots also could complement, and be integrated with, the Einstein 3 program, and existing defense-in-depth cybersecurity capabilities within the Department of Defense, the Department of State, the Department of Justice, and elsewhere.

A third pilot would involve creating a commercial construct and processes that would permit DOD to rapidly acquire operational or technical cyber capabilities from the private sector, to incentivize commercial investments in technology and capabilities, and to facilitate the transition of these capabilities into both government programs and commercial markets. A major goal would be to achieve agility in exploiting innovations and closing vulnerabilities. The committee expects that this pilot would contribute to the cyber acquisition strategy that would be required by sec. 933 of this Act.

The provision would require DOD to conduct a fourth pilot whose purpose would be to develop a process to enable the evaluation and comparison of commercial cyber security products and services across a common set of standards and a common taxonomy. The committee intends that the Department exploit the work of the private sector's development of the Consensus Audit Guidelines and the security controls developed by the National Institute of Standards and Technology. These guidelines and controls are based on the most significant attack patterns, and could form a framework for organizing and integrating commercial products and services.

The committee understands that these pilots will take some time to initiate and complete, but expects the Department to be aggressive, in keeping with the Department's own declared anxiety about the rising cybersecurity threat and the need for forceful corrective action.

John Denning, Director of External Affairs
Office of Cybersecurity and Communications
Department of Homeland Security

Desk: (b) (6)
Secondary: (b) (6)
Back-up: (b) (6)
Pager: (b) (6)
Web: www.dhs.gov/cyber

(b) (6)

From: Butler, Robert J SES OSD POLICY (b) (6)
Sent: Saturday, May 21, 2011 5:19 PM
To: (b) (6)
Subject: Fw: AT&T and Netwitness update
Attachments: AT&T charts

From: Butler, Robert J SES OSD POLICY

Sent: Saturday, May 21, 2011 05:10 PM

To: (b) (6) SES NII/DoD-CIO; (b)(3)-P.L. 86-36 (b) (6) HON OSD POLICY;
 (b) (6)
 (b) (6)
 (b)(3)-P.L. 86-36 (b) (6)

Subject: Fw: AT&T and Netwitness update

(b) (5)

Thanks, Bob

From: (b) (6) (b) (6)
Sent: Saturday, May 21, 2011 10:47 AM
To: (b) (6) 'Gillis, Ryan M' (b) (6)
 (b) (6)
Cc: Carey, Robert J SES NII/DoD-CIO; Guissanie, Gary, SES, NII/DoD-CIO; Butler, Robert J SES OSD POLICY; (b) (6)
 (Intelligence) (b) (6) Agarwal, Sumit SES OSD POLICY; (b) (6) NII/DoD-
 CIO; (b) (6) CIV OSD POLICY (b) (6) (b) (6) HSGAC
 (b) (6) (b) (6) (HSGAC) (b) (6) (b) (6)
 (Appropriations) (b) (6)
Subject: AT&T and Netwitness update

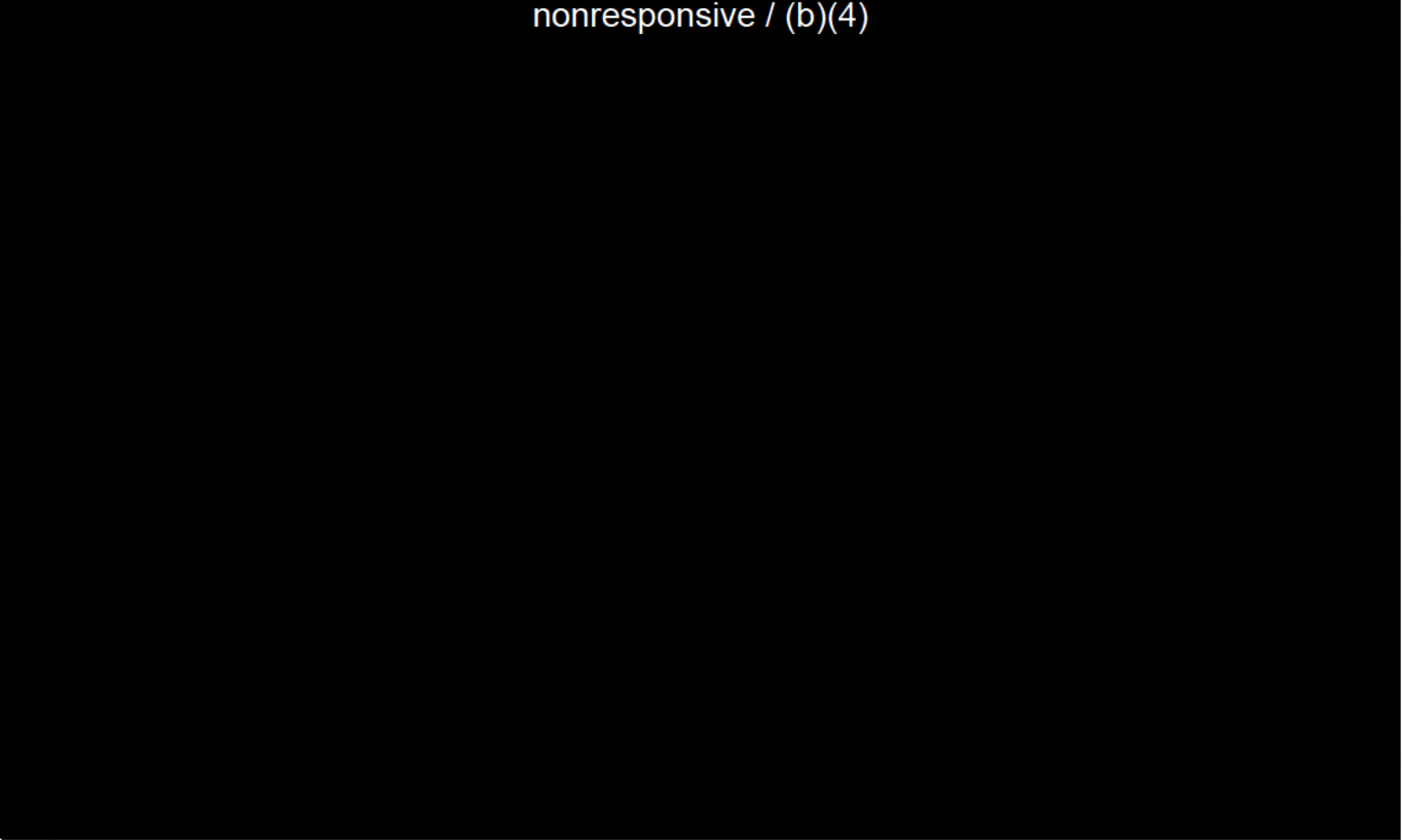
All:

Had a meeting yesterday with AT&T to talk about (1) nonresponsive / (b)(4), and (2) the capabilities they are offering under MTIPS. They brought the attached charts that they pulled from various existing packages – so the page numbering is irrelevant.

This material and what I am going to tell you is proprietary and sensitive.

nonresponsive / (b)(4)

nonresponsive / (b)(4)



(b) (6)

From: McConnell, Bruce
Sent: Thursday, March 31, 2011 11:36 AM
To: Brown, Michael A. RADM; Dean, Nicole M; Stempfley, Roberta
Cc: Ludtke, Meghan; McDermott, Thomas M
Subject: RE: RSVP & security clearance info RE: DIB Opt - In Pilot Meeting, April 4, 2011
Attachments: 20110330 DIB Opt in Pilot Comms Plan MASTER FINAL DRAFT (OSD PA edits) v13 (2)_NSS dhs.docx

(b) (5)

And,

I'll send on the high-side the cleared summary paper. I believe the paper DC will go out next week.

I will add you both to respective email traffic strings the next time something comes across.

As far as operational plans, I have not seen anything more than the summary paper.

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

From: Brown, Michael A. RADM
Sent: Thursday, March 31, 2011 11:12 AM
To: McConnell, Bruce; 'McDermott, Thomas M'; 'Ludtke, Meghan'
Cc: Stempfley, Roberta
Subject: RE: RSVP & security clearance info RE: DIB Opt - In Pilot Meeting, April 4, 2011

Bruce,

Thanks. I forwarded to Nicole. We've not seen any updates on operational plan or how the COAs will actually be executed. We've also not seen any of the paper deputies or other paperwork.

Cheers,
Mike

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: McConnell, Bruce
Sent: Thursday, March 31, 2011 10:53 AM
To: McDermott, Thomas M; Ludtke, Meghan
Cc: Brown, Michael A. RADM; Stempfley, Roberta
Subject: RE: RSVP & security clearance info RE: DIB Opt - In Pilot Meeting, April 4, 2011

Yes, absolutely. Please thank (b) (6) for including us!

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

From: McDermott, Thomas M (b) (6)
Sent: Thursday, March 31, 2011 10:50 AM
To: Ludtke, Meghan; McConnell, Bruce
Subject: FW: RSVP & security clearance info RE: DIB Opt - In Pilot Meeting, April 4, 2011
Importance: High

(b) (5)

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

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

From: (b) (6) DoD OGC (b) (6)
Sent: Thursday, March 31, 2011 10:34 AM
To: 'McDermott, Thomas M'; 'Delaney, David'
Cc: (b) (6) CTR NII/DoD-CIO; (b)(3)-P.L. 86-36 ; (b)(3)-P.L. 86-36 ; (b) (6)
(b) (6) CIV NII/DoD-CIO; (b)(3)-P.L. 86-36 (b) (6) DISL NII/DoD-CIO
Subject: FW: RSVP & security clearance info RE: DIB Opt - In Pilot Meeting, April 4, 2011
Importance: High

(b) (5)

Cheers//RMG

(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) CTR NII/DoD-CIO
Sent: Wednesday, March 23, 2011 4:38 PM
To: (b) (6)
(b) (6)

(b) (6)

(b) (6) (b)(6)-P.L. 86-36
 (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36; (b) (6) DoD OGC; (b) (6)
 HQE NII/DoD-CIO; Guissanie, Gary, SES, NII/DoD-CIO; (b) (6) CIV NII/DoD-
 CIO; (b) (6) CTR NII/DoD-CIO; (b) (6) DISL NII/DoD-CIO;
 (b)(3)-P.L. 86-36 (b) (6) DISL OSD POLICY; (b) (6)
 CTR NII/DoD-CIO; (b) (6) (b) (6) 'Brown Chad Civ DC3'
 Subject: DIB Opt - In Pilot Meeting, April 4, 2011

Dear DIB Partners,

Thank you for participating in last week's teleconference on the DIB Opt-in pilot. As discussed in the teleconference, we will be holding in-person meetings on Apr 4, 2011 to further discuss the way ahead.

DATE/TIME: To help accommodate schedules, two sessions are available, as follows:

- April 4, 2011: 9:00a.m. - 12:00p.m. EST
- April 4, 2011: 1:00p.m. - 4:00p.m. EST

Check-in will occur between 8:00-9:00a.m. and 12:00-1:00p.m.

Please RSVP to (b) (6) or myself (b) (6) and let us know which session your company will be attending. Please include in your RSVP the names of your participants. We welcome the participation of your CIO, CISO and General Counsel staff members at the meeting. Due to space constraints, however, please limit your attendees to 3 participants.

(b)(7)(E), (b)(6)

We look forward to seeing you on the 4th.

Sent on behalf of

(b) (6)

Director, DIB CS/IA