

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

Voluntary Summary Reports Provided by ISPs to NSA in Support of the DIB "Opt-In" Pilot
 October 28, 2011

The ISPs provided voluntary summary reports to NSA during the DIB Pilot. Each ISP provided different information and on different schedules. Below is a description of what information each ISP provided and a sample of each type of report.

AT&T

- Daily report included Green/Yellow/Red status for DNS Sinkholing, Email Filtering and General Infrastructure, or any planned outages. This report did not contain any data.
- During earlier stages of Pilot, no regular weekly reports, but on a few ad hoc occasions provided total # of events for each of the two (b)(3) P.L. 86-36
- On 20 September, at the request of their customers, AT&T began providing weekly summaries of number of DNS hits per domain per day
- On 13 October, AT&T began providing weekly summaries of the number of hits per signature per day for both DNS Sinkholing and Email Filtering
 - o (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

Sample AT&T Report:

Malicious Email Filtering						
10/2	10/3	10/4	10/5	10/6	10/7	10/8
			1			
						36
DNS						
10/2	10/3	10/4	10/5	10/6	10/7	10/8
				1		
						2
				1		
12	8	11	11	15	7	10

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20361001

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

SECRET//

(b)(1) and (b)(3) P.L. 86-36

(b)(4) and (b)(7)

- Weekly DNS Summary report
 - o SIG ID
 - The NSA unique identifier for the signature that triggered the event
 - o Count
 - The number of events triggered during the reporting period for that signature

(b)(4) and (b)(7)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

S Summary Report:

Count

3

29

3

1

- Weekly Email Summary report
 - o SIG ID
 - The NSA unique identifier for the signature that triggered the event
 - o Count
 - The number of events triggered during the reporting period for that signature

(b)(4) and (b)(7)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

ail Summary Report:

Count

5

(b)(4) and (b)(7)

/CenturyLink

- Weekly DNS Detail report contained:
 - o DIB Name (some redacted)
 - Name of the DIB company to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim companies
 - o Host (most redacted)
 - The IP address of the victim host to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim hosts within a company

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

SECRET// (b)(1) and (b)(3) P.L. 86-36

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- Date/Time
 - The date and time at which the event occurred
- Hit Type
 - The level of event correlation that CenturyLink was able to perform
 - Falls into one of the following 3 categories

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

Sample CenturyLink DNS Detail Report:

CTL (b)(4) and (b)(7) DIB DNS Detailed Report - 10/17/11
 Report Date Range = 10/10/2011 12:00:00 GMT TO 10/17/11 12:00:00 GMT

DIB NAME	HOST	(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798	DATE/TIME	(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
REDACTED-2	REDACTED-2		10/11/2011 15:48	
REDACTED-2	REDACTED-2		10/11/2011 15:48	
REDACTED-4	REDACTED-4		10/12/2011 13:10	
UNIDENTIFIED	Not Available		10/12/2011 13:10	
UNIDENTIFIED	Not Available		10/13/2011 18:54	

- Weekly DNS Summary report

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- DIB Name (some redacted)
 - Name of the DIB company to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim companies
- Host (most redacted)
 - The IP address of the victim host to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim hosts within a company
- Safe Hits
 - The number of DNS Sinkholing events categorized with a Hit Type of "SAFE ONLY HIT" or "SAFE & DNS HIT"
- DNS Only Hits
 - The number of DNS Sinkholing events categorized with a Hit Type of "DNS ONLY HIT"

SECRET// (b)(1) and (b)(3) P.L. 86-36

- Total Hits
 - The total number of DNS Sinkholing events

Sample CenturyLink DNS Summary Report:

CTL (b)(1) and (b)(3) DIB DNS Summary Report - 10/17/11

Report Date Range = 10/10/2011 12:00:00 GMT TO 10/17/11 12:00:00 GMT

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

DIB NAME	HOST	SAFE HITS	DNS ONLY HITS	TOTAL HITS
REDACTED-2		1	0	1
REDACTED-2		3	0	3
REDACTED-4		0	1	1

- DNS Hit Correlation Report
 - DATE/TIME (GMT)
 - The date and time at which the event occurred
 - DIB
 - Name of the DIB company to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim companies
 - HASH
 - A one-way hash of the NSA-provided domain associated with the event

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- SAFE DATE/TIME
 - The date and time at which the victim host contacted CenturyLink's safe server (if that activity occurred)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

SECRET// (b)(1) and (b)(3) P.L. 86-36

- DEST IP

- The IP address of the CenturyLink safe server contacted by the victim

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

Sample CenturyLink DNS Correlation Report:

CTL/ (b)(4) and (b)(7) Detailed DIB Report

Report Date Range: 10/10/2011 12:00:00 to 10/17/2011 12:00:00

DATE/TIME (GMT)	DIB	SAFE DATE/TIME
10/11/2011 15:48:19	REDACTED-2	10/11/2011 15:48:19
10/11/2011 15:48:23	REDACTED-2	10/11/2011 15:48:23
10/11/2011 15:48:29	REDACTED-2	10/11/2011 15:48:29
10/11/2011 15:48:34	REDACTED-2	10/11/2011 15:48:34
10/11/2011 20:44:33	REDACTED-5	10/11/2011 20:44:33
10/12/2011 13:10:47	UNIDENTIFIED	10/12/2011 13:10:47

Weekly SMTP Detail report contained:

- DIB Name (some redacted)
 - Name of the DIB company to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim companies
- Hit Date/Time
 - The date and time at which the event occurred
- Server
 - The IP address of the DIB customer mail server to which the malicious email was sent if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique mail servers to which the email was sent
- Attachment Type
 - If the malicious email had an attachment, the type of attachment found

SECRET, (b)(1) and (b)(3) P.L. 86-36

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

(b)(4) and (b)(7)

CTL [REDACTED] DIB Email Hit Detail Report

Date Range: 10/10/2011 12:00:00 to 10/17/11 12:00:00 (GMT)

<u>DIB NAME</u>	<u>HIT DATE/TIME</u>	<u>SERVER</u>	<u>ATTACHMENT TYPE</u>
REDACTED-1	10/11/2011 12:56	REDACTED-1	UNKNOWN
REDACTED-1	10/11/2011 12:57	REDACTED-1	UNKNOWN
REDACTED-1	10/11/2011 13:17	REDACTED-1	UNKNOWN
REDACTED-1	10/11/2011 13:18	REDACTED-1	UNKNOWN
REDACTED-1	10/11/2011 13:58	REDACTED-1	UNKNOWN

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- Weekly SMTP Summary report

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- o DIB Name (some redacted)
 - Name of the DIB company to which the event pertained if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique victim companies
- o Server
 - The IP address of the DIB customer mail server to which the malicious email was sent if authorized by the customer to share, otherwise a "REDACTED-#" placeholder that would distinguish the number of unique mail servers to which the email was sent
- o Total Hits
 - The total number of emails triggered by the specified signature for the specified (or redacted, but unique) customer

(b)(4) and (b)(7)

Sample CenturyLink Email Summary Report:

CTL [REDACTED] DIB Email Hit Summary Report

Date Range: 10/10/2011 12:00:00 to 10/17/11 12:00:00 (GMT)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

<u>DIB NAME</u>	<u>SERVER</u>	<u>TOTAL HITS</u>
Redacted by NSA	Redacted by NSA	3
REDACTED-1	REDACTED-1	12
Redacted by NSA	Redacted by NSA	3

~~TOP SECRET//~~~~(b)(1) and (b)(3) P.L. 86-36~~

DIB Pilot Cybersecurity Assessment

1

(S/ ~~(b)(1) and (b)(3) P.L. 86-36~~) Attachment A –Guidance for
the Protection of Classified Information
Used in ~~(b)(3) P.L. 86-36~~

Last Modified:

31 March 2011

~~TOP SECRET//~~~~(b)(1) and (b)(3) P.L. 86-36~~

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

DIB Pilot Cybersecurity Assessment

2

Contents

1	(U// FOUO) DIB Pilot Security Architecture Purpose.....	3
2	(U// FOUO) Recommendations for Maximized Protection of USG Classified Information	4
2.1	(U) Overall Architecture.....	4
2.2	(U// FOUO) Gateway Function Architecture.....	6
2.2.1	(S//^{(b)(1) and (b)(3) P.L.}) Incoming SMTP Gateway	8
2.2.2	(S//^{(b)(1) and (b)(3) P.L.}) Outgoing DNS Request Gateway	9
Appendix A:	(U// FOUO) (b)(3) P.L. 86-36	11

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~

(b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

3

1 (U) DIB Pilot Security Architecture Purpose

(U//~~FOUO~~) The purpose of the security architecture portion of the network that supports the DIB Pilot processing is to protect the (b)(3) P.L. 86-36 information supplied to the Pilot operational implementers as well as any other equities associated with this information. This document provides a relatively thorough description of the components and configuration that make up the implementation of the (b)(3) P.L. 86-36

~~TOP SECRET//~~

(b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~ // (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

4

2 (U//~~FOUO~~) Recommendations for Maximized Protection of USG Classified Information

2.1 (U) Overall Architecture

(S//~~(b)(1) and (b)(3) P.L.~~) First, consider the following diagram in Figure 1. Without effective boundary control, rogue SMTP or DNS functionality cannot be prevented. The main point here is that each DIB member must:

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

e.g., in the DIB Pilot, this includes incoming SMTP access and outgoing DNS requests) (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

What *can* go wrong *will* go wrong.

(S//~~(b)(1) and (b)(3) P.L.~~) In Figure 1 – which is intentionally sparse because the following diagrams will fill in some important details – DIB Member A has two (perhaps redundant) ISP connections to the Internet. In practice, it is likely that each DIB Member really has many, differently-controlled interfaces at various points in its network – often because of performance considerations (geography, bandwidth, latency and cost).

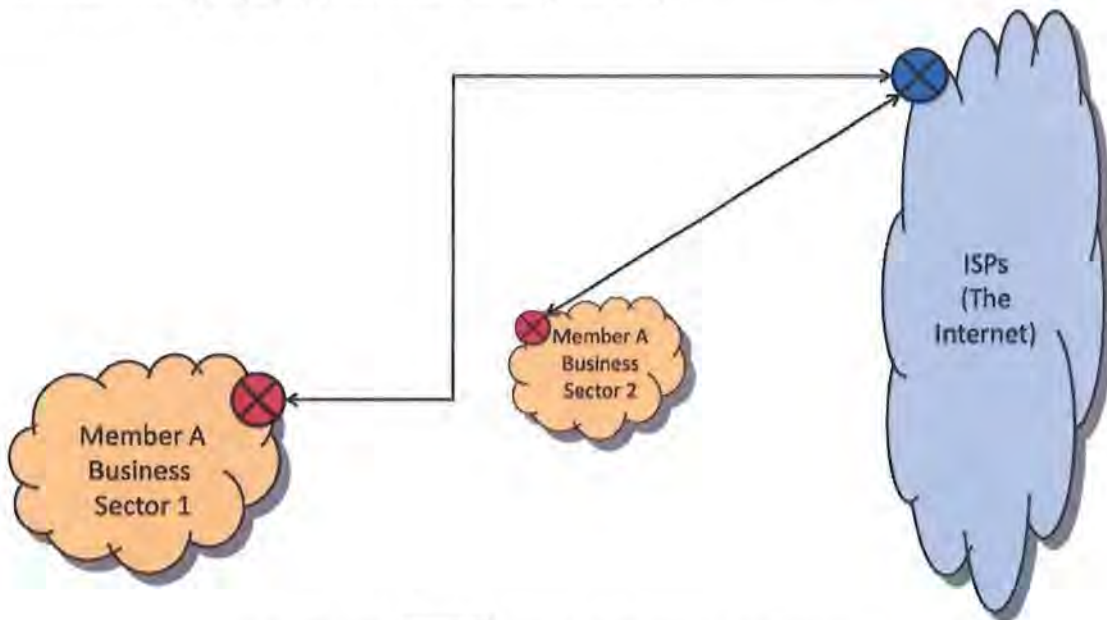


Figure 1 – (S//~~(b)(1) and (b)(3) P.L.~~) Generic DIB Member Architecture

(U) Figure 2 builds on the above basic architecture.

(S//~~(b)(1) and (b)(3) P.L.~~) The salient point here is that in order for each entity to provide commonly-mediated Internet access for the traffic to be protected (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~TOP SECRET~~ // (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~ // (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

5

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

(S) ~~(b)(1) and (b)(3) P.L. 86-36~~ Each member also has the responsibility to ensure that all ISP connections to the commercial Internet are only through ~~(b)(3) P.L. 86-36, (b)(1)~~. Enforcement of this policy – particularly detection of violations – may be problematic, but should be technically feasible. The assurance of such policy is critical.

~~(TS)~~ ~~(b)(1) and (b)(3) P.L. 86-36~~ A critical point of this architecture is that ~~(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~

(in this case, incoming SMTP and outgoing DNS requests) ~~(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~

~~(TS)~~ ~~(b)(1) and (b)(3) P.L. 86-36~~ In this proposed architecture, we name the ~~(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

Figure 2 — ~~(TS)~~ ~~(b)(3) P.L. 86-36, (b)(1)~~ DIB Gateway Architecture

~~TOP SECRET~~ // (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

6

2.2 (U//~~FOUO~~) Gateway Function Architecture~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798 Each gateway must have~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798 We similarly name these

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798 Each gateway should be~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798 Each gateway should~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798 The NSA-provided information should be stored in~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

- (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(TS//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~(S//~~ (b)(1) and (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

7

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~(TS)~~ (b)(1) and (b)(3) P.L. 86-36 (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



The importance of this cannot be overemphasized.

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



(U//~~FOUO~~) Sneaker net is a basic, but secure communications method when used with proper controls. If more real-time processing of system or network element logs should be desired, they would need to be secured according to their security domain considerations.

~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

8

(S//~~(b)(1) and (b)(3) P.L.~~) Administrative staff should perform the following (b)(1), (b)(3) P.L. 86-36, and (b)(3) 18 U.S.C. 798

• Put the server under official change control
(b)(1) and (b)(3) P.L. 86-36

- Quickly restore the host to the desired known state as needed.

2.2.1 (S//~~(b)(1) and (b)(3) P.~~) Incoming SMTP Gateway

(TS//~~(b)(1) and (b)(3) P.L. 86-36~~) The ideal SMTP gateway data flow:

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

9

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



2.2.2 (S) (b)(3) P.L. 86-36, (b)(1) Outgoing DNS Request Gateway

(TS) (b)(3) P.L. 86-36, (b)(1) The DNS request data flow:

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

10

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

11

Appendix A: (U//~~FOUO~~) (b)(3) P.L. 86-36

Table is ~~TS//~~

(b)(3) P.L. 86-36, (b)(1)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~TOP SECRET//~~(b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

Requirements for the Protection of Classified Information – DIB Cybersecurity Initiative

12

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

(b) (6)

From: [REDACTED] a [REDACTED] nd L.
 Sent: [REDACTED] da [REDACTED] b [REDACTED] 6, [REDACTED] 11 [REDACTED] 8 P [REDACTED]
 To: [REDACTED] a [REDACTED] n, [REDACTED] ab [REDACTED]
 Cc: [REDACTED] [REDACTED] [REDACTED] a [REDACTED] . [REDACTED] n [REDACTED] a [REDACTED] nd L.
 Subject: [REDACTED] [REDACTED] [REDACTED] d [REDACTED] [REDACTED]
 Attachments: [REDACTED] [REDACTED] [REDACTED] n [REDACTED] P [REDACTED] n.38 [REDACTED] [REDACTED] 11.d [REDACTED]

CLASSIFICATION: ~~SECRET~~ // **(b)(1) and (b)(3) P.L. 86-36** // ~~20360601~~

CLASSIFICATION: ~~SECRET~~ // **(b)(1) and (b)(3) P.L. 86-36** ~~20360601~~

Attached is the NSA document for starting the discussions with the ISPs.
 The real question is what is DHS's security requirements once we take this initiative over?

Ray Kinstler
 Director, Future Operations, US-CERT

(b) (6)

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

From: Ritz, Daniel W.
 Sent: Tuesday, December 06, 2011 9:28 AM
 To: Bicknell, Wade D.; Willis, Larry E.; Campbell, John; Kinstler, Raymond L.
 Subject: DIB security docs for AT&T

CLASSIFICATION: ~~SECRET~~ // **(b)(1) and (b)(3) P.L. 86-36** // ~~20360601~~

Docs for AT&T...

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

From: **(b)(3) P.L. 86-36**
 Sent: Tuesday, December 06, 2011 8:36 AM
 To: **(b)(3) P.L. 86-36**
 Cc: Goode, Brendan W.; Ritz, Daniel W.; **(b)(3) P.L. 86-36** Harris Daniel G
 NSA-T16 USA CIV; Prather Brian K Mr **(b)(3) P.L. 86-36**

Subject: Resend: RE: (U) DIB security docs for AT&T

Classification: ~~SECRET~~ // **(b)(1) and (b)(3) P.L. 86-36**

(b) (6)

Please replace the NSA Security Requirement for ISP doc with the attached.

The original copy was incorrectly classified as NOFORN.

(b) (6)

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

T1 Net Defense Mission Effect Lead
OPS2A0844

(b) (6)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20360601~~

Classification: ~~SECRET~~ // (b)(1) and (b)(3) P.L. 86-36

DERIVED FROM: NSA/CSSM 1-52

CLASSIFIED BY:

DECLASSIFY ON: ~~20360601~~

DATE OF SOURCE: 20070108

CLASSIFICATION: ~~SECRET~~ // (b)(1) and (b)(3) P.L. 86-36 // ~~20360601~~

DERIVED FROM: NSA/CSSM 1-52

CLASSIFIED BY:

DECLASSIFY ON: ~~20360601~~

DATE OF SOURCE: 20070108

CLASSIFICATION: ~~SECRET~~ // (b)(1) and (b)(3) P.L. 86-36 // ~~20360601~~

DERIVED FROM: NSA/CSSM 1-52

CLASSIFIED BY:

DECLASSIFY ON: ~~20360601~~

DATE OF SOURCE: 20070108

CLASSIFICATION: ~~SECRET~~ // (b)(1) and (b)(3) P.L. 86-36 // ~~20360601~~

SECRET// (b)(1) and (b)(3) P.L. 86-36

NSA Security Requirements for ISP in Support of DIB Security

I. (U) Introduction

(U//FOUO) The purpose of the NSA Security Requirements for the ISP in support of DIB Security is twofold.

- a. (S// (b)(1) and (b)(3) P.L. 86-36) To protect the NSA classified information (b)(1); (b)(3) P.L. 86-36, and (b)(3) 18 U.S.C. 793 NSA SMTP classified signatures and another containing NSA DNS classified signatures.
- b. (S// (b)(1) and (b)(3) P.L. 86-36) To ensure that the security of the communications between the ISP and DIB dealing with either the SMTP or DNS service provided as part of the NSA classified information is accurately conveyed.

(S// (b)(1) and (b)(3) P.L. 86-36) The purpose of the ISP Security Initiative is to protect DIB companies from rogue SMTP or DNS internet traffic. By providing ISPs NSA classified signatures, the ISPs are able to provide additional security capabilities in these two areas to the participating DIB companies that are not available by traditional commercial offerings or products. Therefore, satisfying the above two objectives, protecting NSA classified information and securing the SMTP and DNS service based on the NSA classified signature, is critical to the overall success of this activity. The enclosed requirements must be addressed within the ISP architecture to ensure the above objectives are met.

II. (U) Scope

(S// (b)(1) and (b)(3) P.L. 86-36) This document specifically provides requirements for environments that process DIB SMTP and DNS internet traffic utilizing NSA classified signature information. (b)(1) and (b)(3) P.L. 86-36

(b)(1) and (b)(3) P.L. 86-36 Therefore, the requirements only address ISPs environments providing the SMTP and DNS enhanced services based on NSA classified information. (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 793

(U//FOUO) (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 793

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360601

SECRET// (b)(1) and (b)(3) P.L. 86-36

SECRET//(b)(1) and (b)(3) P.L. 86-36

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

(U//~~FOUO~~) The requirements in this document are based on a notional architecture that provides the necessary layers of defense and devices' security to obtain the stated objectives in section I.

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

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

SECRET//(b)(1) and (b)(3) P.L. 86-36

~~SECRET~~

(b)(1) and (b)(3) P.L. 86-36

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

(U//~~FOUO~~) The requirements cover security needs dealing with physical and logical architecture, Identification and Authentication, Access Control, Auditing/Logging, Security Configuration and Hardening, Services, Management, Network, Cryptography, Key Management Monitoring, Testing, and Documentation. Each of these areas are addressed in the sections below.

III. (U) Document Structure

(S//~~FOUO~~) In order to meet the two security objectives identified in the introduction and to eliminate/reduce the identified threats, security mechanisms are required at various places within the architecture. (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

IV. (U) Requirements

(U//~~FOUO~~) The requirements are written with three levels of criticality. Requirements that are "must haves" to either curtail a threat or support the objectives in section I are notated with the word "**shall**". Requirements that are strongly recommended are notated with the word "**should**". And finally, requirements that would provide another layer of defense and would be "nice to have" are notated with the word "**recommend**" or "**desire**". Italicized sentences are for clarification or further explanation of a requirement.

~~SECRET~~

(b)(1) and (b)(3) P.L. 86-36

SECRET//(b)(1) and (b)(3) P.L. 86-36

a. (U) Architecture

(U//~~FOUO~~) The architecture requirements are split into two overarching categories:

1. (U) Physical

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

SECRET//(b)(1) and (b)(3) P.L. 86-36

~~SECRET//~~



(b)(1) and (b)(3) P.L. 86-36


(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



b. (U) *Devices*

(U//~~FOUO~~) Security functions that support the overall security objectives stated above execute on a variety of devices within this architecture. (b)(3) P.L. 86-36



 Most of these requirements are applicable to all the devices in the architecture that provide security operations in support of the two objectives stated in the introduction. However, in some cases, a requirement is for a specific device. In these cases, a note will be made to indicate the requirement is unique to a particular device. The security functions are: Identification/Authentication, Access Control, Auditing, Security Configuration and Hardening, and Monitoring. By performing these sets of requirements on the appropriate devices within the architecture, the security, thus the objectives, of the system are supported and the threat minimized.

1. (U) *Identification/Authentication*

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

~~SECRET//~~

(b)(1) and (b)(3) P.L. 86-36

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

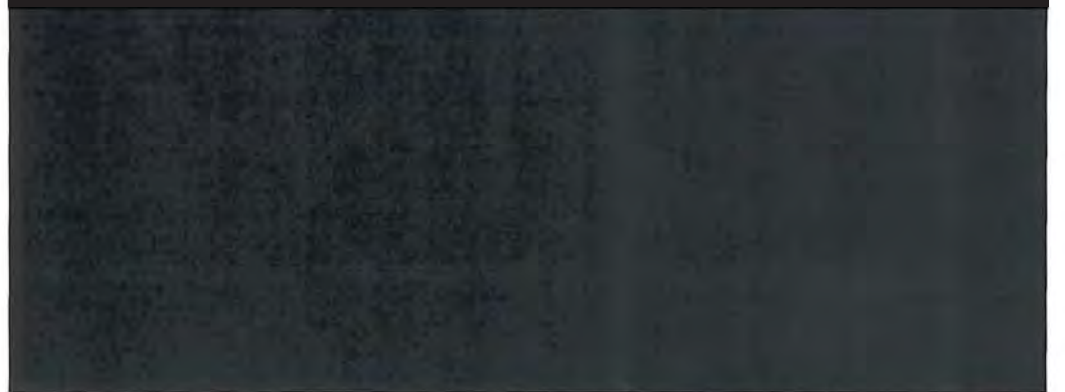

(b)(3) P.L. 86-36



2. (U) Access Control

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

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

~~SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



3. (U) Auditing/Logging

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

~~SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

SECRET// (b)(1) and (b)(3) P.L. 86-36

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

4. (U) Security Configuration and Hardening

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

SECRET// (b)(1) and (b)(3) P.L. 86-36

~~SECRET~~

(b)(1) and (b)(3) P.L. 86-36

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

~~SECRET~~

(b)(1) and (b)(3) P.L. 86-36

~~SECRET~~//

(b)(1) and (b)(3) P.L. 86-36

APPENDIX A

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798



~~SECRET~~//

(b)(1) and (b)(3) P.L. 86-36

(b)(6)

From:

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

Sent:

Monday, 11/11/11 11:11 AM

To:

John A. ...

Subject:

(b)(3) ...

Follow Up Flag:

...

Flag Status:

...

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b)(1) and (b)(3) P.L. 86-36

Thanks,

(b) (6)

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

Deputy General Counsel (Cyber)

National Security Agency

(b) (6)

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

From: [REDACTED]
Sent: [REDACTED]
To: [REDACTED]
Cc: [REDACTED]
Subject: [REDACTED]
Attachments: [REDACTED]
Importance: [REDACTED]

CLASSIFICATION: ~~SECRET~~
 CAVEATS: ~~NOFORN~~
 TERMS: NONE

Summary of legal issues prior to DC prepared by **(b)(3) P.L. 86-36** for DDIR NSA.

(b) (6)

Special Assistant to Deputy Assistant Secretary Cyber Security and Communications

(b)(3) P.L. 86-36, (b) (6)

From: **(b)(3) P.L. 86-36**
Sent: Monday, July 12, 2010 7:32 AM
To: **(b)(3) P.L. 86-36**
Subject: FW: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot
Importance: High

Classification: ~~SECRET//NOFORN~~

From: **(b)(3) P.L. 86-36**
Sent: Saturday, July 10, 2010 9:42 AM
To: [REDACTED]
Cc: [REDACTED]

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

Subject: RE: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot

Classification: ~~SECRET//NOFORN~~

Sir

(b)(3) P.L. 86-36, (b)(1)

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

(b)(1) and (b)(3) P.L. 86-36

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

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

(b)(6)

OPS 1 2C099B

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

From: (b)(3) P.L. 86-36
Sent: Friday, July 09, 2010 7:26 PM
To:
Cc:

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

Subject: RE: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot

Classification: ~~SECRET//NOFORN~~

(b) (6)

Please have this final summary to us first thing Monday morning.

Thank you,

(b) (6)

(on DDIR's account)

(b)(3) P.L. 86-36
Executive Assistant to Deputy Director, NSA
OPS2B, 2B8036; Suite 6242

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

From: (b)(3) P.L. 86-36
Sent: Wednesday, July 07, 2010 7:31 PM
To:
Cc:

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

Subject: RE: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot

Classification: ~~SECRET~~//NOFORN

Sir

[REDACTED]

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

OPS 1 2C099B

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

From: (b)(3) P.L. 86-36
Sent: Wednesday, July 07, 2010 6:52 PM
To:
Cc:

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

Subject: RE: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot

Classification: ~~SECRET~~//NOFORN

(b) (6)

Please follow up the loose ends and give me a final summary that I can take to the Deputies meeting next week. Thanks

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Wednesday, July 07, 2010 5:23 PM
To:
Cc:

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

Subject: (U) Prep for Monday's DC: Response to Legal Issues DOJ Raised Re DIB Pilot

Classification: ~~SECRET//NOFORN~~

Sir

(b)(1) and (b)(3) P.L. 86-36

(b)(1) and (b)(3) P.L. 86-36

From: (b)(3) P.L. 86-36
Sent: Tuesday, July 06, 2010 5:31 PM
To:
Cc:

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

Subject: ** Report from NSS Meeting on DC Read-Aheads **

Classification: ~~SECRET//NOFORN~~

Sir,

(b)(1) and (b)(3) P.L. 86-36

(b)(1) and (b)(3) P.L. 86-36

Sincerely,

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

Director's Special Assistant for Cyber

Chief, NSA Cyber Task Force

Senior Advocate, African American Employee Resource Group

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

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

Classification: ~~SECRET//NOFORN~~

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

OPS 1 2C099B

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20350701~~

Classification: ~~SECRET//NOFORN~~

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20350701

Classification: ~~SECRET//NOFORN~~

DERIVED FROM: NSA
DECLASSIFY ON: ~~x25~~

CLASSIFICATION W/O ATCH: ~~SECRET~~
CAVEATS W/O ATCH: ~~NOFORN~~
TERMS W/O ATCH: NONE

CLASSIFICATION: ~~SECRET~~
CAVEATS: NOFORN
TERMS: NONE

(b) (6)

From: (b)(3) P.L. 86-36
 Sent: [REDACTED]
 To: [REDACTED] a [REDACTED] a [REDACTED] a [REDACTED]
 Cc: [REDACTED] a [REDACTED] (b)(3) P.L. 86-36
 Subject: (b)(3) P.L. 86-36

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Tom

(b)(1) and (b)(3) P.L. 86-36

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

OPS 1 2C099B

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

From: (b) (6)
 Sent: Wednesday, June 30, 2010 10:13 AM
 To: (b) (6) M., Mr., OASD NII; (b)(3) P.L. 86-36
 Cc: (b)(3) P.L. 86-36
 Subject: IPC and DIB Pilot

CLASSIFICATION: UNCLASSIFIED
 CAVEATS: FOUO
 TERMS: NONE

Gentlemen,

(b)(1) and (b)(3) P.L. 86-36

I do not have any additional details, but I assume you heard similarly from your participants. Apparently he also mentioned Thursday's meeting at DOJ and confirmed that OLC would be present.

(b) (6) - I separately forwarded you the list of preliminary questions/discussion topics from DOJ.

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

(b) (6)

CLASSIFICATION: UNCLASSIFIED
CAVEATS: FOUO
TERMS: NONE

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

From:
Sent:
To:
Cc:

(b) (6)
Wednesday, June 30, 2010 11:42 AM
(b)(3) P.L. 86-36 McDermott, Thomas M. (b) (6)
(b)(3) P.L. 86-36
ean, Nicole M.; (b)(3) P.L. 86-36
(b)(3)
Subject: RE: (U) Latest DIB pilot schedule info (U//FOUO)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

Welcome back, and Thanks! Let me ask a couple questions to ensure we're all on the same page:

(b)(3) P.L. 86-36, (b) (5)

Thanks again.

(b) (6)

(b) (6)
Associate General Counsel
DoD Office of General Counsel
Direct
Secure
NIPR:
SIPR:
JWICS

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Wednesday, June 30, 2010 10:39 AM
To: (b) (6); (b) (6)
(b) (6)
Cc: (b)(3) P.L. 86-36
(b)(3) P.L. 86-36 (b) (6) (b)(3) P.L. 86-36
Subject: (U) Latest DIB pilot schedule info

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Tom, Richard, Susan

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

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Friday, June 11, 2011 6:04 PM
To: (b) (6); .GO; Butler, Robert J., Mr., OSD(P); Schaffer, Gregory P.; Dean, Nicole M.; (b)(3) P.L. 86-36; Brown, Michael A. RADM; (b) (6) McDermott, Thomas M.; (b) (6); (b) (6); (b) (6); (b) (6)
Cc: (b)(3) P.L. 86-36
Subject: (U) Follow up to DIB Pilot Discussion

Classification: ~~SECRET~~//NOFORN

(b) (6)

I hope all are well.

At last week's meeting, NSA took two actions to follow up on the exact number of companies participating in the DIB Pilot and the reasons some companies chose not to participate.

1) The final count of companies participating in the DIB Pilot is (b)(7)(b)(3) P.L. 86-36

a.

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

2) Measures of Effectiveness.

As you know, the DIB Pilot is designed to leverage the commercial capabilities of the private sector to improve their ability to monitor, detect and mitigate intrusions and other malicious activity (b)(3) P.L. 86-36 on their networks.

At the conclusion of the operational phase of the Pilot, the participating ISPs and DIB companies may voluntarily provide overall feedback to the USG regarding the progress,

challenges, effectiveness, and other lessons learned to allow for post-Pilot analysis of effectiveness and scalability.

We drafted some measures to determine the effectiveness and scalability of the Pilot's capability to protect against the most sophisticated intrusions - (b)(3) P.L. 86-36

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

3) Below is also further information on the Pilot:

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

All the best,

(b) (6)

*~~(S)~~

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20360201~~

Classification: ~~SECRET//NOFORN~~

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Friday, July 16, 2010 3:54 PM
To: (b) (6) (b)(3) P.L. 86-36 McDermott, Thomas M.
Cc: (b) (6) (b) (6) (b) (6) (b)(3) P.L. 86-36
Subject: (b)(3) P.L. 86-36
(U) RE: DIB Questions (FOUO)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b)(3) P.L. 86-36, (b) (5)

(b)(3) P.L. 86-36 Associate General Counsel (Information Assurance)

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

From: (b) (6)
Sent: Friday, July 16, 2010 3:33 PM
To: (b)(3) P.L. 86-36 (b) (6)
Cc: (b) (6) Bailey, Leonard (JCONTS)
Subject: RE: DIB Questions (FOUO)
Importance: High

CLASSIFICATION: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Are we in a position where we can answer some of the questions attached? This is the information we will need to do a legal review. (b) (6) may have additional thoughts on this. Thanks.

From: (b) (6) (b) (6)
Sent: Monday, June 28, 2010 4:38 PM
To: (b)(3) P.L. 86-36 (b) (6)
Cc: (b) (6)
Subject: DIB Questions

CLASSIFICATION: ~~FOUO~~

Folks,

At the end of last week's meeting we discussed collecting questions and issues that we thought warranted further discussion and circulating them to each other. Attached are some initial questions regarding the DIB project that (b) (6) and I jotted down. They are by no means exhaustive and are only the product of brainstorming between Susan and me. Please circulate to Richard and Maxine, since I don't have their high-side email addresses. Thanks.

(b) (6)

CLASSIFICATION: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Monday, January 03, 2011 5:42 PM
To: McDermott, Thomas M.
Cc: (b)(3) P.L. 86-36
Subject: RE: (U) RE: DIB Pilot Issues

Classification: ~~SECRET~~ (b)(3) P.L. 86-36

Tom,

My understanding is that DOJ (b) (5)
There will be discussion during the session at the svtc tomorrow morning but that is my understanding.

v/r,
MAB

Mike Brown

RADM, USN

Director, Cybersecurity Coordination

National Protection & Programs Directorate

Department of Homeland Security

(b) (6)

From: (b) (6)
Sent: Tuesday, December 28, 2010 11:23 AM
To: (b)(3) P.L. 86-36
Cc: (b)(3) P.L. 86-36
Subject: FW: (U) RE: DIB Pilot Issues

CLASSIFICATION: ~~SECRET~~
CAVEATS: TO

TERMS: NONE

Thomas M. McDermott

Office of the General Counsel

Department of Homeland Security,

National Protection and Programs

(b) (6)

From: McDermott, Thomas M.

Sent: Tuesday, December 28, 2010 11:21 AM

To: Reitinger, Philip R.; McConnell, Bruce W.; Schaffer, Gregory P.; Stempfley, Roberta G.; Brown, Michael A. RADM; Dean, Nicole M.

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

Subject: FW: (U) RE: DIB Pilot Issues

CLASSIFICATION: SECRET

CAVEATS: (b)(3) P.L. 86-36, (b)(1)

TERMS: NONE

Following up on my email from last Wednesday evening, (b) (5)

[REDACTED]

. At a high-level, NSA is proposing:

(b)(3) P.L. 86-36, (b) (5)

Thomas M. McDermott

Office of the General Counsel
Department of Homeland Security,
National Protection and Programs

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Thursday, December 23, 2010 3:07 PM
To: (b) (6); (b)(3) P.L. 86-36 (b) (6)
Cc: Painter, Christopher M.E.; (b) (6) Baker, James A.; (b) (6)
(OIPR); (b) (6) (b) (6) (b) (6), Mr., OGC; Butler, Robert J., Mr., OSD(P);
(b)(3) P.L. 86-36; McDermott, Thomas M.
Subject: RE: (U) RE: DIB Pilot Issues

Classification: ~~SECRET~~ // (b)(3) P.L. 86-36, (b)(1)

Jason et al,

As discussed yesterday, (b) (6)

Happy holidays and best wishes,

(b) (6)

From: (b) (6)
Sent: Wednesday, December 22, 2010 10:55 AM
To: (b)(3) P.L. 86-36; (b) (6)
Cc: Painter, Christopher M.E.; (b) (6) Baker, James A.; (b) (6)
(OIPR); (b) (6) (b) (6) Mr., OGC; Butler, Robert J., Mr., OSD(P)
Subject: RE: (U) RE: DIB Pilot Issues

CLASSIFICATION: ~~SECRET~~ // NOFORN

All:

Here's an informal summary of the Department's agency analysis. (b) (5)

Please contact Jim Baker or me with any questions or concerns about this document.

(b) (6)

Senior Counsel to the Deputy Attorney General

U.S. Department of Justice

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Tuesday, December 21, 2010 6:18 PM
To: (b) (6); (b)(3) P.L. 86-36; (b) (6)
Cc: Painter, Christopher M.E.; Newman, Charles L.; Baker, James A.; (b) (6)
(OIPR) (b) (6) Mr., OGC; Butler, Robert J., Mr., OSD(P)
Subject: (U) RE: DIB Pilot Issues

Classification: ~~SECRET~~

(b) (6)

Thank you for your email and the informal paper tomorrow.

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

As the senior Policy lead for DoD, I'll defer to Bob Butler on the third point.

Adding (b) (6) and Bob Butler to the email chain...

Best,

(b) (6)

From: (b) (6)
Sent: Tuesday, December 21, 2010 5:44 PM
To: (b)(3) P.L. 86-36; (b) (6); (b)(3) P.L. 86-36
Cc: Painter, Christopher M.E.; Newman, Charles L.; Baker, James A.; (b) (6)
Subject: DIB Pilot Issues

CLASSIFICATION: ~~SECRET~~ // ~~NOFORN~~

All:

(b) (5)

(b) (6)

PS -- Can someone at DOD please send this to Bob Butler and (b) (6) I don't have their JWICS addresses.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20351201

Classification: ~~SECRET~~

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20351201

Classification: ~~SECRET~~ / (b)(3) P L 86-36 (b)(1)

DERIVED FROM: NSA/CSSM 1-52

DECLASSIFY ON: ~~20351201~~

CLASSIFICATION W/O ATCH: ~~SECRET~~

CAVEATS W/O ATCH: (b)(3) P L 86-36 (b)(1)

CLASSIFICATION: ~~SECRET~~

CAVEATS: (b)(3) P L 86-36 (b)(1)

TERMS: NONE

DERIVED FROM: MS

DECLASSIFY ON: MR

CLASSIFICATION W/O ATCH: ~~SECRET~~

CAVEATS W/O ATCH: TO

TERMS W/O ATCH: NONE

CLASSIFICATION: ~~SECRET~~

CAVEATS: TO

TERMS: NONE

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Wednesday, November 03, 2010 6:51 PM
To: Dean, Nicole M.
Cc: Schaffer, Gregory P.; (b)(3) P.L. 86-36
 Stempfley, Roberta G.; (b)(3) P.L. 86-36 Delaney, David G.; McDermott, Thomas M.
Subject: (U) RE: DIB

Classification: ~~TOP SECRET~~

Nicole,

Thanks for the note - my folks have left for the day, but I'll forward the "final" version tomorrow - it incorporates DHS's second round of comments and the draft language David, Richard and the attorneys worked. So, nothing new there.

Re: the second item - what I said today was that the ISPS had provided their security architectures for security review and that the security team had reviewed it and done an assessment (b)(3) P.L. 86-36

I didn't attend those meetings, as we were just interested in the outcome not the detailed technical discussions, but I can ask the team for whatever architecture details they received, if that is valuable to you. Please let me know.

Re: the status meetings, we established weekly status meetings last week. We had one each with AT&T and (b)(4) and (b)(7). The one with (b)(4) and (b)(7) this week was cancelled at their request, because there were no technical updates to provide. As we discussed, you are welcome to attend and you have the days and times. As you heard today, the legal issues drive the pace of the operational decisions, so in some cases, meetings are cancelled if legal progress has not been made and we are forced to slow the operational progress to keep the two parallel.

Best,

(b) (6)

From: (b) (6)
Sent: Wednesday, November 03, 2010 4:47 PM
To: (b)(3) P.L. 86-36
Cc: Schaffer, Gregory P.; (b)(3) P.L. 86-36 (b)(3) P.L. 86-36 (b)(3) P.L. 86-36 (b)(3) P.L. 86-36
 Stempfley, Roberta G.; (b)(3) P.L. 86-36 (b)(3) P.L. 86-36 McDermott, Thomas M.
Subject: DIB

CLASSIFICATION: ~~TOP SECRET~~
 CAVEATS: ~~NOFORN~~
 TERMS: NONE

(b) (6)

At the IPC you mentioned

(b) (5)

(b) (5)

On a separate note, I realize the status meetings with the ISPs you had scheduled this week were cancelled, however, if there are any other meetings DHS can engage on with respect to the DIB pilot, please let me know. We want to ensure we stay as closely sync'd as possible.

Thanks so much,

Nicole

DERIVED FROM: ms
DECLASSIFY ON: ms

CLASSIFICATION: ~~TOP SECRET~~
CAVEATS: NOFORN
TERMS: NONE

Classification: ~~TOP SECRET~~

(b) (6)

From: (b)(3) P.L. 86-36
 Sent: Thursday, June 10, 2010 2:10 PM
 To: (b)(3) P.L. 86-36
 Cc: (b)(3) P.L. 86-36 (b) (6) Ryan
 Subject: RE: (U) Invitation to DIB Pilot (b) (6) Meetings

CLASSIFICATION: UNCLASSIFIED
 CAVEATS: FOUO
 TERMS: NONE

Thank you, (b) (6). Tom McDermott (cc'd here) is handling the operational issues related to the DHS "design study" work with ISPs under CNCI 3. For continuity on those topics (and since I'll be on leave or jury duty for a significant part of the coming weeks) I'm looping him in to attend the NSA-DOD meetings with vendors if possible.

I have not yet seen a timeline or description of the DOD DIB pilot study plan. Would DOJ attend these meetings too, or is there a different series of meetings that they would join?

Thanks.

(b) (6)

(b) (6)

From: (b)(3) P.L. 86-36
 Sent: Wednesday, June 09, 2010 3:37 PM
 To: (b)(3) P.L. 86-36
 Cc: (b)(3) P.L. 86-36

(b) (6) (b)(3) P.L. 86-36
 Subject: (U) Invitation to DIB Pilot Technical Exchange Meetings

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

David

This is to invite you to the technical exchange meetings NSA is holding with carriers starting Friday, 11 June from 9-11 a.m. with (b)(4) and (b)(7) and continuing Fri 1-3 p.m. with ATT, both in room 2A0218. The meeting with (b)(4) and (b)(7) will be Wed, 16 June from 1-3 p.m. Meetings with

the remaining 3 Tier I carriers are being scheduled. We are waiting confirmation that carrier attorneys will be attending.

These are what we are envisioning as the "first round" of meetings during which (b) (5)

The second round will be for (b)(3) P.L. 86-36, (b) (5)

A second round meeting with ATT is scheduled for 22 June 10-12 a.m.

Please let me and (b)(3) P.L. 86-36 know if you are planning on attending. Hope to see you there.

(b)(3) P.L. 86-36, Associate General Counsel (Information Assurance)

Subject to attorney-client privilege. Do not release outside NSA without OGC approval.

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CLASSIFICATION W/O ATCH: UNCLASSIFIED

CAVEATS W/O ATCH: ~~FOUO~~

TERMS W/O ATCH: NONE

CLASSIFICATION: UNCLASSIFIED

CAVEATS: ~~FOUO~~

TERMS: NONE

(b) (6)

From: (b)(3) P.L. 86-36
(b)(3) P.L. 86-36
Sent: Friday, August 05, 2011 5:31 PM
To: Goode, Brendan W.; (b)(3) P.L. 86-36
Dean, Nicole M.; McDermott, Thomas M.;
Stempfley, Roberta G.; (b) (6)
Subject: (U) RE: Summary of DHS Notes on the DIB Participant Meeting (2-Aug)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Brendan,

Thanks. We'll review and share our notes.

As an aside, we've been giving a lot of thought to

(b) (5)

We've acknowledged their points and are thinking about how to correct that in the future, welcome your thoughts,

Best,

(b) (6)

From: (b) (6)
Sent: Friday, August 05, 2011 3:00 PM
To: (b)(3) P.L. 86-36
Cc: (b)(3) P.L. 86-36 Dean, Nicole M.; McDermott, Thomas M.; (b)(3) P.L. 86-36
Stempfley, Roberta G.; Taran, Gabriel
Subject: Summary of DHS Notes on the DIB Participant Meeting (2-Aug)

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

Hi (b) (6)

I am passing along our notes from Tuesday's session with the DIB participants. Sorry for the delay getting to you my notes for the meeting summary. Also, I couldn't find Victoria's e-mail address; please feel free to pass this along to her as well.

Below are the key points that we took away. When do you anticipate the draft meeting notes would be ready?

(b) (5)

(b) (5)

Let me know if you have any questions on my inputs. I will be out of the office Monday-Thursday and will have limited access to JWICS. Please let me know at my low-side account (b) (6) if you have any questions or if I need to find a JWICS terminal to see your response.

Thanks,

(b) (6)

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Holzer, James V.

From: (b)(3) P.L. 86-36
Sent: Tuesday, May 04, 2010 5:04 PM
To: Reitinger, Philip R.; Schaffer, Gregory P.; Broxon, Michael A.; McConnell, Bruce W.
Cc: McDermott, Thomas M.; (b) (6)
Subject: DIB pilot update

CLASSIFICATION: ~~SECRET~~
CAVEATS: ~~NOFORN~~
TERMS: NONE

Gentlemen,

(b)(1), (b)(5)

(b) (6)

DERIVED FROM:
DECLASSIFY ON:

CLASSIFICATION: ~~SECRET~~

CAVEATS: ~~NOFORN~~

TERMS: NONE

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

NSA Final Recommendation on AT&T Architecture

(U//~~FOUO~~) Below are a list of items that NSA believes must be done to the AT&T architecture in order to protect the signatures from a variety of potential threats. These recommendations are in no specific order since they are all equally important to the security of the signatures.

~~(S)~~ (b)(1) and (b)(3) Recommendation 1: (b)(1); (b)(3) P.L. 86-36, and (b)(3) 18 U.S.C. 798
~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
[Redacted]

~~(S)~~ (b)(1) and (b)(3) Recommendation 2: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
[Redacted]
~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
[Redacted]

~~(S)~~ (b)(1) and (b)(3) Recommendation 3: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
[Redacted]
~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
[Redacted]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20370301

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

~~(S)~~ (b)(1) and (b)(3) Recommendation 4: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Recommendation 5: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Recommendation 6: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Recommendation 7: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Recommendation 8: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Rationale: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~(S)~~ (b)(1) and (b)(3) Recommendation 9: AT&T provided a new (b)(1); (b)(3) P.L. 86-36, and (b)(3) 18 U.S.C. 798. However, we have several questions. We believe that a meeting about this would be beneficial to all parties.

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

Meeting notes from DIB briefing to [REDACTED]

15 June 2010

Date of Meeting: 6/16/2010

Time: 1300-1500

(b) (2)

ISP: (b)(4) and (b)(7)

(U//~~FOUO~~) Overview: Presentation briefed collectively by (b)(1) P.L. 86-36

[REDACTED] The same basic script as described in previous meeting notes was followed as the previous meetings with (b)(4) and (b)(7) AT&T, and (b)(4) and (b)(7)

~~(S//~~ (b)(1) and (b)(3) P.L. 86-36 (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~(S//~~ (b)(1) and (b)(3) P.L. 86-36 (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798~~(S//~~ (b)(1) and (b)(3) P.L. 86-36 (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798(U//~~FOUO~~) (b)(4) comments centered on:

- (U//~~FOUO~~) What exactly is the govt asking and are they being asked for the same thing at DHS concerning EINSTEIN
- ~~(S//~~ (b)(1) and (b)(3) P.L. 86-36 They own one of the largest free public DNS infrastructures that could be leveraged (b)(1) P.L. 86-36
- (U//~~FOUO~~) They explained their capabilities are centered on detection and analysis on their customer networks while they perform higher end redirection and mitigation of traffic on their internal (b)(4) networks.
- (U//~~FOUO~~) They also mentioned that all of the ISPs share malicious IPs once a month.

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

Meeting notes from DIB briefing to (b)(4) and (b)(7)

15 June 2010

Date of Meeting: 6/15/2010

Time: 1300-1500

(b) (2)

ISP: [REDACTED]

(U//FOUO) Overview: Presentation briefed collectively by (b)(3) P.L. 86-36

[REDACTED] The same basic script was followed as the previous meetings with (b)(4) and (b)(7) and AT&T.

1. (U//FOUO) (b)(3) P.L. 86-36 [REDACTED]
2. (U//FOUO) NSA provided a list of questions to (b)(4) and (b)(7) (each ISP will be provided a copy) querying them on cyber protection offerings and strategies

3. (S//FOUO) (b)(3) P.L. 86-36 [REDACTED]

(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

4. (U//FOUO) The briefing also contains a slide describing all of the interfaces for the partner system; there is also an accompanying document that describes the interfaces in detail
 - a. NSA told (b)(4) and (b)(7) that they would be provided both the briefing and the interface document
 - b. We could definitely use this information and should be provided to us
5. (U//FOUO) (b)(3) P.L. 86-36 [REDACTED]
6. (U//FOUO) NSA told (b)(4) and (b)(7) that E3 and the DIB are asking for exactly the same thing; the only difference is the protected customer base and the terminology is different.
 - a. Both sides are being directed to have joint engagements in the future.

7. (U//FOUO) (b)(3) P.L. 86-36 [REDACTED]

8. (U//FOUO) (b)(3) P.L. 86-36 [REDACTED]

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

9. (U//FOUO) (b)(3) P.L. 86-36

Additional items:

(S//~~(b)(1) and (b)(3) P.L. 86-36~~) Only one of the ~~(b)(1) and (b)(3)~~ participants was at the meetings down here. Same basic soundtrack as to what the govt is asking the ISPs to consider. (b)(3) P.L. 86-36

(TS//~~(b)(1) and (b)(3) P.L. 86-36~~) (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36Notes for Technical Exchange Meeting (TEM) #1 with Tier 1 ISPs for Protection of the DIB

Date of Meeting: 6/11/2010

Time: 0900-1100

(b) (2)

ISP: (b)(4) and (b)(7)

(U//FOUO) Overview: Presentation briefed collectively by (b)(3) P.L. 86-36

(U//FOUO) Anne presented the following:

(b) (5)

(U//FOUO) Under CYBERCOM, DIRNSA has authority over the ".mil" and DIB areas. DHS has the responsibility for the ".gov" and critical infrastructure.

(S//~~FOUO~~) Next, Steve briefed the (b)(3) P.L. 86-36 piece. Anne indicated that the ISPs needed to indicate what pieces of the (b)(3) P.L. 86-36

(U//FOUO) Lastly, Pat briefed the concept of operations which necessary in order to build the current defensive capability. (b)(3) P.L. 86-36

(TS//~~FOUO~~) (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798
(b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

(U//FOUO) (b)(3) P.L. 86-36

(U//FOUO) (b)(3) P.L. 86-36

(U//FOUO) Questions (from (b)(4) and (b)(7)) Answers (from NSA):

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

- 1) **Question #1:** What is the relationship of the DIB partners (basically, will the DIB partners be thought of as customers or participants)?

a. **Answer #1:** DIB partners will definitely be involved.

- 2) **Question #2:** Will this effort lead to a RFP?

a. **Answer #2:** (b)(3) P.L. 86-36

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

(U//FOUO) Other Items:

- 1) (b)(4) and (b)(7) requested additional information from (b)(3) on Cloud (i.e., a paper written by (b)(3)).
- 2) (b)(3) stated the urgency of getting this effort done.
- 3) The 60-day legal/operational framework timeline began on 6/4/2010.
- 4) Slides presented showed a joint effort with DHS/NSA.
- 5) A set of questions were provided to (b)(4) and (b)(7) for follow-on discussion at the 2nd TEM (dates listed below) for homework assignments. The set of questions included the following:
 - a. (U//FOUO) What are the services you provide clients with under the various categories of "managed security services"?
 - b. (U//FOUO) What types of malicious network activity mitigation actions do you currently perform to maintain your network? Please provide a level of operational detail for a couple of mitigation examples used today (b)(3) P.L. 86-36
 - c. (U//FOUO) How is the effectiveness of mitigation actions measured, both qualitatively and quantitatively?
 - d. (U//FOUO) In support of network security, what types of monitoring (at any and all levels) is currently performed?
 - e. (U//FOUO) What network or threat information is useful to you in support of your detection and mitigation operations?

~~TOP SECRET//~~ (b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

- f. (U//~~FOUO~~) If government classified information is to be supplied in support of network security operations, please describe the mechanism(s) currently in place, if any, that will protect such information.
 - g. (U//~~FOUO~~) Please walk through the classified scenario briefed during the first TEM, describing how you would implement the various functions within your own architecture. Which functional elements would you implement on your own, in partnership with government capabilities or would be required to be performed by the government partner?
- 6) Next TEM #1 meetings:
- a. 6/11/2010 (Fri): 1300-1500 with AT&T
 - b. 6/15/2010 (Tue): 1300-1500 with (b)(4) and (b)(7)
 - c. 6/16/2010 (Wed): 1300-1500 with [REDACTED]
 - d. 6/17/2010 (Thurs): 900-1100 with [REDACTED]
 - e. 6/17/2010 (Thurs): 1300-1500 with [REDACTED]
- 7) Tentative 2nd TEM (TEM #2) Meetings:
- a. 6/22/2010: 0900-1100 with AT&T

Scenarios:

(TS// (b)(1) and (b)(3) P.L. 86-36) DIB project is looking at 2 scenarios: (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

[REDACTED]

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

TOP SECRET//(b)(1) and (b)(3) P.L. 86-36Meeting notes from DIB briefing to (b)(4) and (b)(7)

15 June 2010

Date of Meeting: 6/15/2010

Time: 1300-1500

(b) (2)ISP: (b)(4) and (b)(7)**(U//FOUO) Overview:** Presentation briefed collectively by (b)(3) P.L. 86-36The same basic script was followed as the previous meetings with (b)(3) and AT&T.

1. **(U//FOUO)** NSA commented that the USG will be responsible for any QOS degradation due to the implementation of any DIB protection (b)(4) and (b)(7)
2. **(U//FOUO)** NSA provided a list of questions to (b)(4) and (b)(7) (each ISP will be provided a copy) querying them on cyber protection offerings and strategies
(b)(3) P.L. 86-36
3. **(S//(b)(3) P.L. 86-36)** (b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
4. **(U//FOUO)** The briefing also contains a slide describing all of the interfaces for the partner system; there is also an accompanying document that describes the interfaces in detail
 - a. NSA told (b)(4) and (b)(7) that they would be provided both the briefing and the interface document
 - b. We could definitely use this information and should be provided to us
5. **(U//FOUO)** (b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
6. **(U//FOUO)** NSA told (b)(4) and (b)(7) that E3 and the DIB are asking for exactly the same thing; the only difference is the protected customer base and the terminology is different.
 - a. Both sides are being directed to have joint engagements in the future.
7. **(U//FOUO)** (b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
8. **(U//FOUO)** (b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36
(b)(3) P.L. 86-36

TOP SECRET//(b)(1) and (b)(3) P.L. 86-36

~~TOP SECRET~~// (b)(1) and (b)(3) P.L. 86-36

9. (U//~~FOUO~~) (b)(3) P.L. 86-36

Additional items:

(S//~~FOUO~~) Only one of the (b)(4) and (b)(7) participants was at the meetings down here. Same basic soundtrack as to what the govt is asking the ISPs to consider. (b)(3) P.L. 86-36

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

(TS//~~FOUO~~) (b)(1); (b)(3) P.L. 86-36; and (b)(3) 18 U.S.C. 798

// (b)(1) and (b)(3) P.L. 86-36

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Monday, June 04, 2012 12:11 AM
To: (b)(3) P.L. 86-36
Cc: (b)(7) P.L. 86-36
Subject: (U) NSA response to ACTIONS from DHS/NSA (b)(4) and (b)(7) telecon on
Attachments: Conference Call Notes 31 May 2012.docx; DIB_ISP_DNS_Sigs_pro Final OFFICIAL SIGNED DOC for release to ISPs.docx
Follow Up Flag: Follow up
Flag Status: Flagged

Classification: (b)(1) and (b)(3) P.L. 86-36

(b) (6)

>From my perspective, our telecon was productive as many (b)(4) and (b)(7) questions were answered. NSA is working on timely answers to a couple questions that arose requiring additional investigation. Attached are 2 classified (SECRET// (b)(4) and (b)(7) documents in response to (b)(4) and (b)(7) request and written response (in blue text, yellow text is open items) to the questions we received from (b)(4) and (b)(7). We will try to provide timely response to the outstanding questions through high-side email, but if DHS (b)(4) and (b)(7) requests a follow-on meeting for clarification, NSA will be available. Once (b)(4) and (b)(7) architecture is finalized, we should meet to make sure everyone is on the same page.

v/r, John

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

TD PM for DHS-NSA DECS/E3A Program

OPS2A 2A0844: (b) (6)

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

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

367-3023(s)

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

NBP322 (Hours: Fri AM)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20370201

Classification: SECRET// (b)(1) and (b)(3) P.L. 86-36

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36**(U) Protections for DNS signatures at ISPs****(U) Introduction:**

~~(S)~~ [REDACTED] Currently, the Defense Industrial Base (DIB) security initiative is using two (b)(3) P.L. 86-36 to protect the DIB companies. These two capabilities provide classified signatures for SMTP and DNS. For this discussion, the DNS signatures are the concern. (b)(1); (b)(3) 18 U.S.C. 798 and (b)(3) P.L. 86-36

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~(S)~~ [REDACTED] (b)(1); (b)(3) 18 U.S.C. 798; and (b)(3) P.L. 86-36

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U//FOUO) (b)(1); (b)(3) 18 U.S.C. 798; and (b)(3) P.L. 86-36

[REDACTED]

[REDACTED]

(U) Risks:

(U//FOUO) (b)(3) P.L. 86-36

[REDACTED]

[REDACTED] the following describes items that an adversary could do.

(U) An adversary can:

- [REDACTED] (b)(1); (b)(3) 18 U.S.C. 798; and (b)(3) P.L. 86-36
- [REDACTED]
- [REDACTED]

- (S// [REDACTED] (b)(1); (b)(3) 18 U.S.C. 798; and (b)(3) P.L. 86-36
- [REDACTED]

(U) PROCEDURAL OVERVIEW

(U) Below are the high level steps needed in preparing signatures, the sequence for operational compare and the algorithms that can be implemented now, stressing that they are currently insecure

~~SECRET~~ (b)(1) and (b)(3) P.L. 86-36

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

because all crypto-processing is in the clear. Therefore, additional layered security mechanisms are required to reduce the risk to the signature list.

(U) Signature preparation:

(U) Upon receipt of the DNS signatures, the following steps shall be taken:

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

(U) Query handling:

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

(U) "Encryption" methods:

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

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

SECRET//~~(b)(1) and (b)(3) P.L. 86-36~~

(U) Review of proposals

(U//FOUO) ~~(b)(3) P.L. 86-36~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- **(U) Hardening and Filtering**

- ~~(S//~~ ~~(b)(3) P.L. 86-36, (b)(3) 18 USC 798, (b)(1)~~
- [REDACTED]
- [REDACTED]

- ~~(S//~~ ~~(b)(3) P.L. 86-36, (b)(3) 18 USC 798, (b)(1)~~
- [REDACTED]
- [REDACTED]
- [REDACTED]

- **(U) IPSEC**

- ~~(S//~~ ~~(b)(3) P.L. 86-36, (b)(3) 18 USC 798, (b)(1)~~
- [REDACTED]
- [REDACTED]

- ~~(S//~~ ~~(b)(3) P.L. 86-36, (b)(3) 18 USC 798, (b)(1)~~
- [REDACTED]

(U//FOUO) ~~(b)(3) P.L. 86-36~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Conclusion:

(U) To provide a more secure solution, the ISP vendors if placing the DNS signature in enclave 1 shall choose one of the three options to better protect the signatures. These options are only to be used for

SECRET//~~(b)(1) and (b)(3) P.L. 86-36~~

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

systems that meet the "NSA Security Requirements for ISP in Support of the DIB Security" or any revision to this requirements document.

~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

(b) (6)

From: (b)(3) P.L. 86-36
Sent: Thursday, November 04, 2010 4:09 PM
To: Dean, Nicole M.
Cc: Scaffer, Gregory P.; (b)(3) P.L. 86-36
 Stepfley, Roberta G.; (b) (6) (b)(3) P.L. 86-36 McDerott, Thomas M.; (b)(3) P.L. 86-36
 (b) (6) (b)(3) P.L. 86-36
Subject: (U) E DIB
Attachments: DIB Cybersecurity Plan_Final.doc
Categories: Purple Category

Classification: ~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36

Nicole,

As requested, attached is the final version of the DIB Pilot Plan.

Best,

(b) (6)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20350701~~

Classification: ~~SECRET~~/(b)(1) and (b)(3) P.L. 86-36