Defense Industrial Base Pilot Cybersecurity Plan

(U) DIB Pilot Cybersecurity Plan

Table of Contents

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350701

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

(U) DIB Pilot Cybersecurity Plan

1 (U) Executive Summary

(U//~~FOUO~~) Congress and the President have assigned the Department of Homeland Security (DHS) important responsibilities for protection of critical infrastructure from cyber and physical threats. Similarly, the Congress and the President have assigned the Department of Defense (DoD) important responsibilities for protection of DoD information and defense information infrastructure, and within the above construct, as the Sector Specific Agency for Defense Industrial Base (DIB) critical infrastructure protection activities.

The Department of Defense relies on the Defense Industrial Base (DIB) for many key functions, from fundamental research, acquisition and logistics to design and support of its command and control networks. The DIB represents a growing repository of DoD information and intellectual property on unclassified networks. As DoD's capabilities and the security of the Nation are inherently dependent on the security and integrity of information in the DIB, both DHS and DoD recognize that additional initiatives must be developed to rapidly increase the level of cybersecurity protection for the DIB to a level equivalent to DoD's unclassified network.

~~(S/~~[redacted] Through the National Security Agency, the Department of Defense has developed a way to provide an active perimeter defense capability to protect its unclassified networks from what it believes to be the most harmful cyber threats. DHS is currently looking at options for leveraging this defense capability to protect Federal Executive Branch civilian networks as part of its EINSTEIN 3 efforts. [redacted]

(U//~~FOUO~~) This DIB Pilot Cybersecurity Plan establishes the operational, legal, technical, and acquisition frameworks necessary for Tier 1 Internet Service Providers (ISPs) to rapidly implement classified cyber threat (b)(3) P.L. 86-36 in order to protect participating DIB companies in a manner consistent with DoD's protection of its unclassified networks. The methodology employed for this plan is driven by four key objectives: (a) the pilot must be implemented within a short timeframe (within eight weeks of approval of this Plan e.g. November 1) and operated for 60-90 days; (b) the pilot operations must include the deployment of substantive classified capability to mitigate existing and future threats; (c) the capability must be scalable to DIB entities of varied network defense capability and resources; and (d) the Plan's operational framework must be fully transparent and address privacy and civil liberty concerns.

(U//~~FOUO~~) Key highlights of the plan include:

- The Pilot will build on existing DoD/DIB Cyber Security/Information Assurance (CS/IA) program Framework Agreements (FA) to share cybersecurity information in accordance with existing DoD authorities. Participating DIB companies will request that the ISPs provide these services and share information with DoD/NSA as an addendum to established Framework Agreements.[1]
- The DIB Pilot may also provide key experience and lessons learned that could inform the design of a broader national strategy to protect the nation's critical infrastructure. Consistent with DHS's overall authority and responsibility for protecting the nation's critical infrastructure and enhancing non-federal cybersecurity, any significant change to the DIB pilot beyond the -current proposal, would be agreed to-DHS and expansion into other sectors would be led by DHS.
- The Pilot will implement two of the core defensive techniques used by DoD today to protect the Non-classified Internet Protocol Router Network (NIPRNet) / .mil network domain. These techniques protect against adversary methodologies used in a large number of documented intrusions today (beaconing to adversary command and control servers and malicious emails).
- The Pilot is intended to be an enhancement to commercial services that ISPs make available to commercial customers[2], including the DIB, and is intended to augment, not replace, the DIB participants' current security measures.
- The Pilot is intended to rely on voluntary informed consent of the DIB companies and their users.
- DoD/NSA will share classified cyber threat signatures (b)(3) P.L. 86-36 with participating Tier 1 ISPs. DoD/NSA will also have a process and an ability to include signatures (b)(3) P.L. 86-36 provided by DHS in accordance with DHS cybersecurity and infrastructure protection authority.
- Participating Tier 1 ISPs will operate NSA and DHS provided signatures [redacted] on behalf of the participating DIB companies on DIB company traffic only. **The U.S. Government (USG) will not be monitoring any DIB communications.**
- The participating Tier 1 ISPs may use the (b)(3) P.L. 86-36 signatures and technical assistance only for the benefit of their participating DIB clients. Participation in this pilot is voluntary. This Plan is based on the premise that the USG will not pay the ISP's for their participation in the Pilot.

Consistent with its role in leading the national effort to protect critical infrastructure and improving the Nation's cybersecurity posture, the Department of Homeland Security is a key partner with the Department of Defense in the DIB Pilot. As noted above, the Pilot may also provide key insights into future DHS efforts to protect the Nation's critical infrastructure and enhance non-federal Cybersecurity..

[1] Department of Defense Instruction 5205.13 Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities, dated January 29, 2010.

[2] While the ISPs offer security services, none of their potential participating DIB companies currently subscribe to these services.

2 (U) Background

(U//~~FOUO~~) Defense Industrial Base networks, including those critical to DOD and the Armed Forces, continue to experience substantial intrusions and data exploitation from a wide array of state and non state actors. The impact of these intrusions on the Department's missions is significant as more than 80% of its logistics are transported by private companies and mission critical systems are designed, built and often, maintained by defense contractors. As a result, the military's mission critical networks are not neatly bounded by those ending in .mil; the DoD relies on private sector networks and capabilities to field and fuel troops and weapons in battle. Ensuring that its partners' networks are secured is a key concern for the Departments of Defense and Homeland Security, because adversaries will find the weakest link and exploit it, whether it is a DoD or DIB partner network.

(U//~~FOUO~~) Sophisticated and Significant Compromise of and Threats to Defense Industrial Base Networks:

- (~~S~~//(b)(3) P.L. 86-36, (b)(1)
- (~~S~~//(b)(3) P.L. 86-36, (b)(1)
- (U//~~FOUO~~) During the period August 2007-August 2009, the Defense Cyber Crime Center's (DC3's) Defense Computer Forensics Lab (DCFL) performed deep dive intrusion forensics on 38 terabytes of media to support a law enforcement investigation of significant intrusions into private sector organizations. The targets included (b) (7)(E organizations, most with a nexus to the DoD as defense contractors; others included universities with a DoD research relationship or private companies whose networks were exploited as an unwitting hop point to the former. The DCFL processed the 38 terabytes in 116 technical examinations and in 102 cases confirmed compromise sufficient to establish admin level access or lesser forms of command & control.
- (~~S~~//(b)(3) P.L. 86-36, (b)(1)

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

(U//~~FOUO~~) The above provides evidence that: DIB networks are high value targets for U.S. cyber adversaries; DoD efforts to secure and defend sensitive military information needs to extend to critical networks within the Defense Industrial Base; and, providing the Defense Industrial Base with access to DoD technologies and highly classified [redacted] techniques will significantly increase their ability to secure and defend their networks against sophisticated cyber threats.

(U//~~FOUO~~) The Defense Industrial Base is comprised of over 10,500 companies, of which over 8,000 are cleared defense companies. Of these 8,000 cleared companies, approximately 2,500 have facilities that are approved for storage of classified information. The DIB ranges from large multi-sector corporations with significant technical capability and resources to smaller, less cybersecurity capable companies. The Pilot's scope is limited to the (b) (7)(E) DIB participants in the Defense Industrial Base Cyber Security/ Information Assurance program. Common network hygiene is a key component of effective network security. However, the intrusion and exploitation techniques used by sophisticated adversaries (including foreign intelligence services) often are undetectable by standard, commercial defensive measures. As a result, protecting against the most sophisticated threats requires highly advanced capabilities.

3 (U) The DIB Pilot Cybersecurity Plan

3.1 (U) Operational Description

(U) On 4 June, 2010, the Deputy Secretary Defense requested that the Director of NSA *"...develop a DIB Security initiative... beginning with the development of a detailed plan for a pilot program to provide DoD's active perimeter defense capability in conjunction with commercially available internet, network or other communications services available for use by the DIB. Please work with the Department of Homeland Security and others as appropriate... The activities described above will be undertaken pursuant to the Department's information assurance authorities, and in furtherance of the Department's ongoing DIB Cyber Security/Information Assurance and Critical Infrastructure Protection activities."*

(U) The methodology used in this "plan for a pilot program", described below, is driven by four key objectives:

1. The pilot must be implemented within a short timeframe (Fall 2010) and extend for 60-90 days (speed to implementation)
2. The pilot must include the deployment of substantive capability to mitigate existing threats
3. The approach must be scalable to DIB entities of varied network defense capability and resources

4. The Plan's operational framework must be fully transparent and address privacy and civil liberty concerns.

(U//~~FOUO~~) Based on its technical expertise, NSA has determined that working with Tier 1 internet service providers (ISPs) is the most efficient way to accomplish the goals outlined in the Deputy Secretary of Defense's memorandum. "Tier 1 ISP" is an industry term that refers to an ISP that does not lease bandwidth from other providers, which means that Tier 1 ISPs own and operate the architecture through which all internet traffic, including malicious traffic, traverses. There are a relatively small number of Tier 1 ISPs, dozens of Tier 2 ISPs, and hundreds of Tier 3 ISPs.

(U) Four Step Approach for the DIB Cybersecurity Pilot

1. (~~S//~~[redacted]) Identify mechanisms for integrating (b)(1) within the Tier 1 ISP networks by leveraging commercial security technologies and capabilities.
    a. (b)(3) P.L. 86-36, (b)(1)
        iv. voluntarily elects to participate in the planning and pilot efforts;
        v. is willing to provide statistics and summary information to the U.S. Government;
    b. Identify the cyber threats associated with the willing corporate entity and cross check them against available (b)(3) P.L. 86-36 Select two classified (b)(3) P.L. 86-36 to be implemented over a 60-90 day pilot.
2. (~~S//~~[redacted]) Build the operational and legal frameworks necessary for
    a. The DoD and DHS (through DoD) to share the appropriate intelligence, signatures, (b)(3) P.L. 86-36 with the participating ISP,
    b. The participating ISP to implement the (b)(3) P.L. 86-36 for the participating DIB entity(ies)
    c. The participating DIB company to amend its Framework Agreement with DoD and consent to the ISP sharing its information (i.e., reports of mitigated intrusions into DIB networks) with the USG, through DoD. DoD will then share appropriate, anonymized information with DHS.
3. (U//~~FOUO~~) Implement and test the plan in a 60-90 day pilot for participating DIB companies.
4. (U//~~FOUO~~) Post pilot period, work with DHS and other appropriate entities to analyze effectiveness, scalability of the pilot capability and determine lessons learned for follow on phases to protect a larger number of Defense Industrial Base entities with a broader range of (b)(3) P.L. 86-36

3.2 (U//~~FOUO~~) Identification and Selection of DIB Pilot Scenarios

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

Based on this analysis and a thorough review of the capabilities the ISPs already offer as part of their managed security services, the following two (b)(3) P.L. 86-36 were identified for the pilot: *DNS Sinkholing* and *Malicious Email Filtering*. The following sections describe each of the (b)(3) P.L. 86-36 and the corresponding information flow.

3.2.1 (U//~~FOUO~~) Scenario 1 – DNS Sinkholing

(U//~~FOUO~~) Domain Name Service (DNS) is a mechanism by which a domain name, such as "www.acq.osd.mil", is translated to its network address. It is analogous to looking up the phone number for a business in the yellow pages. (b)(3) P.L. 86-36

(U//~~FOUO~~) The figure below depicts the steps by which DNS Sinkholing is accomplished by the ISPs:

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

DNS Sinkholing Scenario

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

Figure 1 – DNS Sinkholing

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

(~~S~~/[redacted]) During the pilot period, participating ISPs will:

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

3.2.2 *(U//~~FOUO~~) Scenario 2 – Malicious Email Filtering*

~~(S/~~[redacted] The second (b)(3) P.L. 86-36 to be implemented in the pilot is "Malicious Email Filtering." (b)(3) P.L. 86-36, (b)(1)

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

Malicious Email Filtering Scenario

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

Figure 2 – Malicious Email Filtering

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

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

~~(S//~~[redacted] In implementing this (b)(3) P.L. 86-36, the ISPs will:

- Adapt current commercially available technologies that can protect the classified DoD and DHS information provided by the DoD
- (b)(3) P.L. 86-36, (b)(1)
- Aggregate & disclose reports of (b)(3) P.L. 86-36 activity as described in Section 3.2.3 below.

3.2.3 (U) Information Data Flow

(U//~~FOUO~~) As part of the operational construct for the pilot, there are four notional paths for the flow of information: 1) From USG to ISP; 2) From ISP to DIB; 3) From ISP to USG, and 4) from USG to DIB. These four information paths are described in detail below for each of the two countermeasure scenarios.

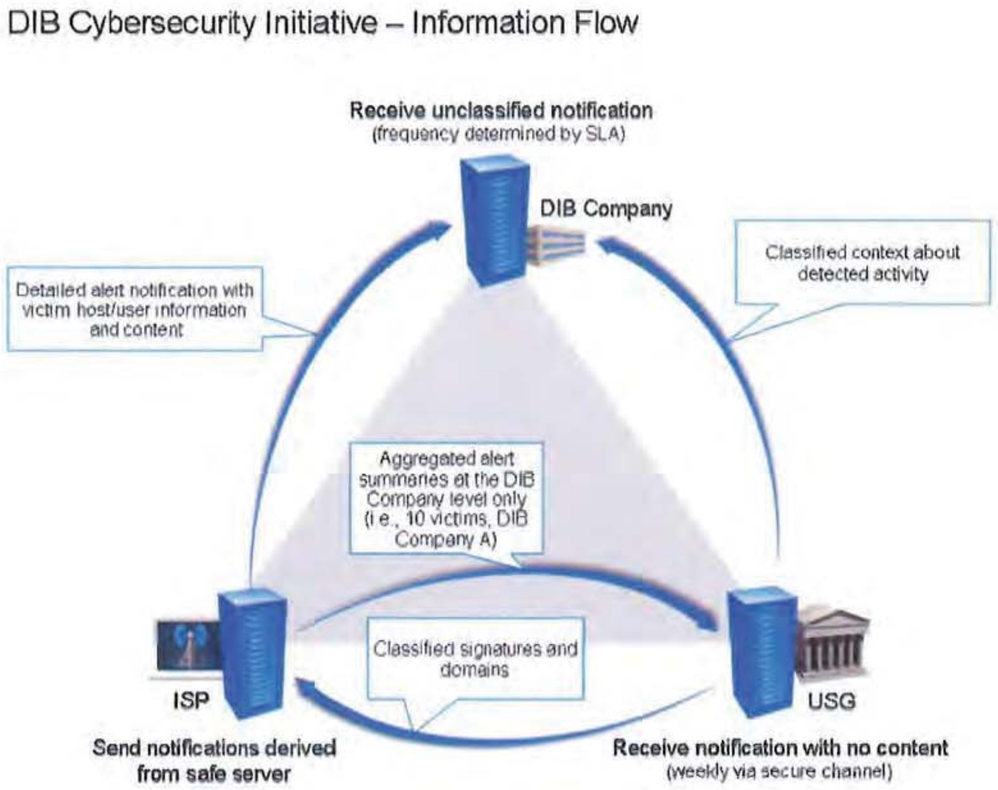
DIB Cybersecurity Initiative – Information Flow
Receive unclassified notification
(frequency determined by SLA)
DIB Company
Detailed alert notification with victim host/user information and content
Classified context about detected activity
Aggregated alert summaries at the DIB Company level only (i.e., 10 victims, DIB Company A)
Classified signatures and domains
ISP
USG
Send notifications derived from safe server
Receive notification with no content
(weekly via secure channel)

Figure 3 – Depiction of Recipients of Various Types of Information

3.2.3.1 (U//~~FOUO~~) DNS Sinkholing Information Flow

3.2.3.1.1 (U//~~FOUO~~) From USG to ISP

(~~S~~//[redacted] The USG, through DoD, will provide the ISPs with a list of classified malicious domains, safe server configurations, and supplemental signatures. DHS will also provide supplemental signatures (b)(3) P.L. 86-36 to DOD for sharing with the ISP.

3.2.3.1.2 (U) From ISP to DIB

(U//~~FOUO~~) The ISPs will provide DIB companies information in the manner and time defined by their Service Level Agreement (SLA). The expectation is that the ISPs will provide near real-time unclassified alert information directly to the DIB Company. For descriptions of the specific data elements the ISP companies expect to provide to participating DIB entities, please reference Appendix C.

3.2.3.1.3 (U//~~FOUO~~) From ISP to USG

(~~S~~/[redacted] On an aggregated basis, the ISPs will provide periodic reports to the USG, through DoD. For the pilot, the expectation is that the reports will be provided weekly and that the information will be sent using secure channels. The DOD Defense Cyber Crime Center will receive the information for their subsequent analysis and provision of cross-participant reporting (as is done under the current DIB CS/IA Framework Agreements. DoD will provide a copy of these reports to DHS, in accordance with the Framework Agreements and DHS authority under Title II of the Homeland Security Act and HSPD-7. For descriptions of the specific data elements to be provided to DoD and DHS, please reference Appendix C.

3.2.3.1.4 (U) From USG to DIB

(~~S~~/[redacted] On a case-by-case basis, DoD (via DC3) may provide additional classified information to DIB companies related to the alerts they received from their ISP. This may include information provided to DoD by DHS. Any additional information will not be real-time, but will provide context related to the observed activity contained in the aggregated reports the ISPs provided. The information might be for a specific DIB company alerted to an incident, or could be aggregated and anonymized to ensure it is appropriate for distribution to all signatories of the DoD CIO's Framework Agreement in the DIB CS/IA Program.

(U//~~FOUO~~) This plan does not otherwise impact the information or other activities under the DoD CIO's Framework Agreement with the DIB participants in the DIB CS/IA program.

3.2.3.2 (U//~~FOUO~~) Malicious Email Filtering Information Flow

3.2.3.2.1 (U//~~FOUO~~) From USG to ISP

(~~S~~//[redacted] Using secure channels, the USG, through DoD, will provide classified signatures that serve as indicators of malicious content in email. The signatures, which may include signatures provided to DoD by DHS, will be thoroughly tested and vetted as high confidence indicators on which the ISPs can take immediate action.

(U//~~FOUO~~) Based on activity reported back from the ISPs and as part of its normal mission, DoD will provide updated DOD and DHS signatures and will request the removal of signatures that are no longer relevant throughout the course of the pilot.

3.2.3.2.2 (U) From ISP to DIB

(U//~~FOUO~~) The ISPs will provide DIB companies information in the manner and time defined by their Service Level Agreement (SLA). The expectation is that the ISPs will provide near real-time unclassified alert information directly to the DIB Company. For descriptions of the specific data elements to be provided in the Malicious Email Filtering scenario, please reference Appendix D.

3.2.3.2.3 (U//~~FOUO~~) From ISP to USG

(~~S~~//[redacted]) On an aggregated basis, the ISPs will provide periodic reports to the USG, through DoD, at the DIB Entity level only. The reports will not include information identifying the individual infected machine within the DIB company, the report will only identify the targeted DIB company (i.e. no information regarding individual DIB company employees or email recipients will be included). (b)(3) P.L. 86-36, (b)(1) DoD will provide a copy of these reports to DHS, in accordance with the Framework Agreements and DHS authority. Subsequent analysis by DHS will further DHS's overall responsibilities to protect the nation's critical infrastructure. For descriptions of the specific data elements to be provided to DoD and DHS in the Malicious Email Filtering scenario, please reference Appendix D.

3.2.3.2.4 (U) From USG to DIB

~~(S//~~[redacted]) On a case-by-case basis, DC3 and/or DHS, through DoD, may provide additional classified information to DIB companies related to the alerts they received from their ISP, in accordance with the existing DIB Cyber Security Framework Agreements. (b)(3) P.L. 86-36, (b)(1)

(U//~~FOUO~~) This plan does not otherwise impact the information shared with DIB participants under the DoD CIO's Framework Agreement in the DIB CS/IA Program. DC3 will continue to provide the same information and summarized reporting that is currently offered under the Framework Agreements.

3.2.3.2.5 (U) Additional Information Flows

(U//~~FOUO~~) Although not part of the operational data flow as a result of applying the (b)(3) P.L. 86-36 there will be a separate data flow between a) the DIB to the ISP and b) the DIB to DoD.

3.2.3.2.5.1 (U) From DIB to ISP

(U//~~FOUO~~) Prior to initiating the pilot, each DIB company and its ISP will review their Service Level Agreement to ensure that the appropriate level of DIB company and user consent is in place.

3.2.3.2.5.2 (U) From DIB to DoD

(U//~~FOUO)~~ Each participating DIB company will amend its Framework Agreement with DoD specifying that it requests the ISP to provide these services and share the cybersecurity intrusion information from the pilot with the USG (through DoD~~,~~ who will forward to DHS). This plan does not affect the existing requirement of DIB signatories to the Framework Agreement to report intrusion incidents to DC3. Participants should continue to engage that office as they normally would. If, during the course of the pilot, any participant believes it has discovered false positives, justifying information can be shared with DoD and DHS via DC3 and appropriate analysis will be done in a timely manner.

3.2.4 (U) Evaluation Methodology

(U//~~FOUO~~) The DIB Pilot is expected to provide enhanced security for the DIB participants, as well as improved situational awareness to DoD and DHS about nation state targeting of DIB companies, as well as the extent to which the tools, techniques, and infrastructure overlaps with those targeting networks for which DoD and DHS have responsibilities to protect. Following approval of the Plan, an Evaluation Methodology to determine the effectiveness and scalability of the Pilot will be developed in collaboration with the participating ISPs and DIB companies, DHS, and other appropriate entities. The Evaluation Plan will be distributed to the DIB pilot participants at the start of the pilot and used at the conclusion of the Pilot to determine the strategy for any follow on phases.

3.2.5 (U) Protection of Classified Information

(~~S~~/[redacted] In order for the participating Tier 1 ISPs to protect DoD information residing on or transiting DIB company networks using DoD's most sensitive information, they must demonstrate the ability to adequately protect USG sources and methods. This will be achieved through a variety of methods:

- The ISPs will maintain all classified information in secure compartmented information facilities (SCIFs) accredited to store the level of information provided and only appropriately cleared personnel will have access to the systems storing the classified signatures.
- Security best practices will be observed throughout the design of the operational architecture for each ISP. (b)(3) P.L. 86-36 NSA is working with Certification and Accreditation authorities and the ISPs to develop an implementation that affords suitable protection of government classified information for the DIB Pilot scenarios.

(b)(3) P.L. 86-36 [redacted]

- The ISPs will share only unclassified information directly with DIB customers. All classified information that is shared with the DIB participants will be handled via approved channels in the current DIB CS/IA program.

Providing classified information to ISPs – who will use this information to mitigate threat – is a key component of this plan. As part of the implementation phase of the pilot, DoD and DHS will work with the ISP's to develop a Counter Intelligence Plan outlining steps to be used to identify potential targeting of this information by foreign adversaries.

3.3 (U) Legal Description

(U//~~FOUO~~) (b)(3) P.L. 86-36, (b) ( ) [redacted]

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

[redacted]

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

3.4 (U) Acquisition/Business Framework

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

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

3.4.1 (U) Business Model

The purpose of the DIB Cyber Security Initiative pilot is to partner with commercial ISPs to provide a proof of concept demonstration to rapidly improve the network security of participating DoD's Defense Industrial Base partners in order to protect DoD information residing on or transiting on critical DIB networks. This approach fuses the intelligence driven techniques DoD uses to secure military networks with similar commercial managed security services employed by ISPs for their own networks or on behalf of their commercial customers. To scope the pilot, an initial market assessment was performed to identify Tier 1 ISPs' existing technical capabilities and to determine the capabilities that could be deployed in the near term.

3.4.2 (U) Internet Service Providers (ISPs)

(U//~~FOUO~~) As previously mentioned, there are a relatively small number of Tier 1 ISPs and many Tier 2 and Tier 3 ISPs. Tier 2 and Tier 3 ISPs purchase transit service from one or more of the Tier 1 ISPs. Although there is no authoritative list of ISPs by these Tiers, organizations such as Cooperative Association for Internet Data Analysis (CAIDA) names six U.S. owned Tier 1 ISPs—AT&T, (b)(4) (b)(4) (b)(4) (b)(4) and (b)(4)

3.4.2.1 (U) ISP Down-select

(U//~~FOUO~~) Invitations to participate in Technical Exchange Meetings (TEMs) were sent to the six U.S. Tier 1 ISPs (AT&T, (b)(4) and (b)(7) declined the invitation to meet with NSA (b)(3) P.L. 86-36 During the first TEM with the ISPs, NSA provided briefings on network defense.

(U//~~FOUO~~) Following the initial TEMs, a formal letter was sent to the five remaining ISPs requesting written confirmation of their intent to participate in the planning of the

DIB Pilot. The letter also included a request for a written response to a set of detailed questions regarding their technical capabilities, conceptual business model and timelines for implementation of the proposed scenarios in the DIB pilot. Written intent to participate indicated agreement to meet the minimum criteria required to participate as detailed below:

1. Possession of the capability to accept and manage classified information by the period of the follow on pilot (September – November 2010).
2. Capability to participate fully in the pilot by implementing the two capabilities during the period of the pilot (November 2010).

(U//~~FOUO~~) In addition, to allow for meaningful participation in the planning efforts and follow on pilot activity, within the specified time frames, the working team determined that it was a critical requirement that the ISP's also satisfy the following two additional criteria:

3. ISP acts as a provider to at least one participating DIB company.
4. ISP has provided sufficient detailed technical information to permit evaluation of its proposed implementation of the two scenarios.

(~~S~~//[redacted]) The following chart summarizes the results of the analysis for each ISP using the four enumerated selection criteria:

	AT&T	(b)(4) and (b)(7)
Criteria 1	(b)(3) P.L. 86-36	
Criteria 2		
Criteria 3		
Criteria 4		

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

(U//~~FOUO~~) Based on the evaluation of all the responses received against the established criteria for participation, AT&T, (b)(4) and (b)(7) were selected as the Tier 1 ISPs for the DIB pilot. (b)(3) P.L. 86-36

(~~S~~//[redacted] (b)(3) P.L. 86-36

3.4.2.1.1 (U) Business Relationship with ISP

~~(S~~//[redacted] DoD and/or NSA will enter into a Memorandum of Understanding (MOU) with each of the (b) (7)(E) [redacted] selected ISPs for the implementation of this DIB Pilot activity. ISP participation in the DIB Pilot is voluntary; (b)(3) P.L. 86-36, (b)(1) [redacted] The MOU and associated statement of expectations will define the sharing of USG (b)(3) P.L. 86-36 [redacted] threat information with Tier 1 ISPs, document the approval to implement those [redacted] by the ISP for the protection of participating DIB company traffic during the pilot, and document the reporting by the Tier 1 ISP to the DIB and to the USG for the duration of the pilot.

3.4.2.1.2 (U) Impact of Pilot

(U//~~FOUO~~) DIB companies may have business arrangements with more than one of the participating Tier 1 ISP. DIB companies may select to participate with one or more of those ISPs, as they deem appropriate.

3.4.3 (U) Defense Industrial Base Entities (DIB)

(U//~~FOUO~~) (b)(3) P.L. 86-36 [redacted] DoD already has cyber security relationships with DIB partners, namely the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) program managed by ASD(NII)/DoD CIO. In accordance with DoD Instruction 5205.13, dated January 29, 2010, the DIB CS/IA is intended to enhance cybersecurity protection of critical defense information and programs on DIB unclassified networks through a variety of mechanisms, including bilateral sharing of classified cyber threat information and cyber security best practices, cyber intrusion reporting, forensics analysis, and damage assessments. Under this program, ASD(NII)/DoD CIO oversees the DIB CS/IA program and related DoD Cyber Crime Center (DC3) activities. As of June 1, 2010, (b) (7)(E) [redacted] DIB companies had signed Framework Agreements (FA) under the DIB CS/IA program. The DIB CS/IA Framework Agreements address the pivotal issues for facilitating bilateral information sharing, intrusion reporting, forensics analysis and damage assessments, and authorize the secure sharing of Government threat products with third-party network security/service providers. Because the DIB Pilot and the DIB CS/IA program share a common purpose of improving the protection of critical defense information carried on unclassified DIB networks, the same criteria that were used to identify DIB CS/IA participants was deemed valid for selection of DIB companies for this DIB Pilot.

(U//~~FOUO~~) As a result, on June 30, 2010, the Acting ASD(NII)/DoD CIO issued an invitation to the (b) (7)(E) [redacted] DIB CS/IA partners to participate in a briefing and discussion on the pilot to determine their interest in voluntarily participating in the planning and pilot.

[redacted]

3.4.3.1 (U) DIB Participation

(U//~~FOUO~~) Of the (b) (7)(E) DIB companies invited, (b) (7)(E) agreed to participate in one or more briefing sessions. Following those discussions, the DIB partners were asked to confirm their interest in continuing to participate in planning for a pilot. (b) (7)(E) DIB companies who attended opted in to the planning efforts. The remaining (b) (7)(E) declined to participate, citing limited resources or the fact that they receive service through a non-Tier 1 ISP.

(U//~~FOUO~~) The (b) (7)(E) DIB companies and the (b) (7)(E) participating ISPs then participated in sessions where DoD provided a brief overview of the pilot (b)(3) P.L. 86-36 the standardized reporting construct, and the legal framework.

(U//~~FOUO~~) The criteria for a DIB company to participate in the pilot are:

- Subscribe to service from one of the (b) (7)(E) participating Tier 1 ISPs
- Execute Framework Agreement addendum by the period of the pilot
- Negotiate modified service level agreement(s) (SLA) with their Tier 1 ISP(s) by the period of the pilot

(U//~~FOUO~~) All DIB partners who meet the above criteria may opt in to participate in the pilot. There will not be a limit or a further down-select process. Due to the complexity of negotiating changes to existing SLAs, companies have notified us that they will not finalize these changes or confirm their participation prior to approval of the DIB Cybersecurity Initiative Plan.

3.4.3.2 (U) DIB Partner Business Relationship

(U//~~FOUO~~) Participation by the DIB partner in this pilot is purely voluntary. If a partner chooses to opt in to the pilot, it will sign an addendum to the existing DIB CS/IA Framework Agreements that will describe the scope of the pilot and document the DIB company responsibilities for reporting to DoD for the duration of the 60-90 day pilot. There should be no change to the existing information sharing and reporting relationship under the DIB CS/IA.

(U//~~FOUO~~) The DIB company will negotiate modification of its Service Level Agreement (SLA) to the ISP to address the implementation by the ISP of the enhanced (b)(3) P.L. 86-36 on their company networks for the duration of the 90 day pilot. While these SLAs are between the ISP and DIB partner, NSA/DoD have developed standardized reporting requirements (data fields and periodicity) between the ISP and DIB partner to ensure consistency of the ISPs' managed security services during the initial pilot. Although outside the scope of the Government's involvement, it is DoD's understanding that the participating ISPs will not charge additional fees (above the current managed security service charges under the existing SLAs) for the duration of the pilot.

3.5 (U) Impact of Pilot

(U//~~FOUO~~) NSA has not identified any potential risks associated with this effort that could jeopardize existing DoD - DIB cybersecurity activities at this time.

4 (U) Role of DHS in the DIB Pilot Operational Framework

(U//~~FOUO~~) The following core principles describe the DoD approach to the DIB Pilot with respect to DHS responsibilities to coordinate the overall national effort to enhance the protection of critical infrastructure and lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, state and local governments, and the private sector to protect critical infrastructure:

- The DIB Pilot is a limited scope, proof of concept initiative fueled by the urgency of the threat to DIB networks and the impact on DoD's mission and assets of delay.

- It is DoD's intention and belief that the DIB Pilot should support and in no way challenge DHS's authorities and its implementation of EINSTEIN 3 or efforts to enhance nonfederal cybersecurity and protect critical infrastructure.

- DoD has no intention to grow this pilot as a substitute to EINSTEIN 3. Indeed, any follow on phases will only be designed in full partnership with DHS.

- The DIB Pilot will provide key experience and lessons learned that may inform the design of a broader national strategy, led by DHS, to protect the nation's critical infrastructure.

- DoD and DHS are committed to mutual transparency with regard to the implementation of the DIB Pilot.

(U//~~FOUO~~) DHS Role in the Operational Framework for the DIB Pilot

DHS and DoD have identified three areas for close partnership and collaboration within the operational framework of the DIB Pilot consistent with existing DHS authority set forth in Title II of the Homeland Security Act, HSPD-7, and HSPD-23.

- Providing Cyber Threat Information: DHS will provide DoD with threat signatures and other classified threat information to enrich those DoD provides to the ISPs.

- Sharing Alert Information: DoD will provide DHS alert information generated within the DIB Pilot, in accordance with the Framework Agreements and DHS authority.

- Governance. The DIB Pilot involves carefully scoped addenda to existing DoD-DIB cyber information sharing arrangements in order to enable the DIB companies to enhance the security of unclassified networks critical to DoD. Consistent with DHS's overall authority and responsibility for protecting the nation's critical infrastructure and enhancing non-federal cybersecurity, any significant changes to the DIB Pilot beyond the current proposal~~,~~ would be agreed to by DHS and expansion into other sectors would be led by DHS

5 (U) Relationship with Existing Efforts

5.1 (U) DIB Cyber Security / Information Assurance (CS/IA) Program

(U//~~FOUO~~) In 2007, in response to evidence of compromises of DoD unclassified weapons, technology and combat support information resident on, or transiting, DIB unclassified networks, the Deputy Secretary of Defense directed the establishment of DoD's DIB CS/IA program. This program is voluntary and is focused on building and maintaining close partnerships with industry to contend with advanced persistent cyber threats.

(U) The DIB CS/IA program provides the mechanisms to exchange relevant cyber threat and vulnerability information in a timely manner; provides intelligence, operational and digital forensic analysis on threats; supports cyber intrusion damage assessments for information compromised on DIB unclassified networks; and expands government/industry cooperation, while ensuring that industry equities and privacy are protected.

(U//~~FOUO~~) The proposed DIB Pilot with ISPs is designed and intended to augment current cyber security activities in the DIB CS/IA program. In addition, the information derived from the pilot potentially will provide additional understanding of adversary tactics, techniques and procedures (TTPs). For example, (b)(3) P.L. 86-36 [redacted]

5.2 (U) EINSTEIN 3

~~(S~~//(b)(3) P.L. 86-36, (b)(1) DHS' EINSTEIN 3 design activities and the DoD DIB Pilot will both leverage the ISPs to protect .gov and DIB traffic and therefore are pursuing a similar strategy. EINSTEIN 3's area of focus is protecting the traffic of USG Executive Branch Agencies; the DoD DIB Pilot's area of focus is protecting private sector entities housing DoD information in Defense Industrial Base networks. (b)(3) P.L. 86-36 [redacted] involve the largest Internet Service Providers (ISPs), and require NSA technical expertise and support to complete.

(U//~~FOUO~~) The DIB Pilot is focused on assessing, and later piloting, the most rapid, efficient technical and operational infrastructure for enhancing the security services provided by the Tier 1 ISPs, in methodical, progressive phases. The pilot, outlined in this Plan, was carefully scoped to exclude government provided capabilities or rapid linkages with the USG which introduce additional legal, policy or technical complexity. Hence, although the Pilot will implement two of the core defensive techniques used by DoD today to protect the Non-classified Internet Protocol Router Network (NIPRNet) / .mil network domain, it will not implement the full set of defensive techniques used.

(~~S~~//[redacted] The EINSTEIN 3 design activity will analyze the inherent capabilities of each of the ISPs in order to understand how each ISP can provide DoD network defense capabilities in a managed service environment. Additionally, the design activity will define an acquisition strategy to implement the managed service capabilities through a spiral development approach. This approach provides the opportunity to incorporate lessons learned from the DIB pilot during their engagements with the ISPs as well as provide feedback on DHS lessons learned during their engagements with NSA. The overlapping schedules of the two activities have not posed a risk to the progress of Comprehensive National Cybersecurity Initiative (CNCI) Initiative #3, rather, they provide an environment for leveraging lessons learned and provide a potential resource savings to the Government. To date, the ISPs have suggested designs that would satisfy requirements for both efforts.

(U//~~FOUO~~) A core group of technical personnel assigned to the DIB Pilot are also working on the joint NSA/DHS EINSTEIN 3 Design Team. The team shares information across both activities, ensuring that both activities can leverage both sets of lessons learned.

5.3 (U) Oversight of Protection of Privacy/Civil Liberties

(U//~~FOUO~~) The choice of only two of the core defensive techniques deployed by DoD to protect its unclassified networks and the concomitant limitation of scope of the DIB Pilot effort reflects the Department's desire to protect the privacy and civil liberties of DIB entity users. There are currently a number of ongoing discussions in Interagency forums on the most appropriate oversight mechanisms for E3 and related efforts, like the DIB Pilot.

DoD will work with such interagency bodies to identify and implement the most appropriate oversight mechanism for the DIB Pilot prior to instantiation of the Pilot (November 2010).

6 (U) Strategy for Follow-On Phases

(U//~~FOUO~~) The first phase of this effort was carefully scoped with a focus on speed to implementation, operational security, scalability and privacy and civil liberty concerns. If the pilot is successful, there is significant potential to expand the protection of sensitive DoD information within critical DIB networks through subsequent phases that add both breadth of coverage (i.e., number of ISPs and DIB participants) and depth of threat mitigation (b)(3) P.L. 86-36 Any expansion of the pilot will be agreed to by DHS and coordinated with other appropriate entities, and will likely present additional legal issues which will need to be researched and carefully analyzed. Furthermore, a phased approach will allow for the application of lessons learned from careful assessment of the effort as it progresses - starting with the Pilot activity and including each subsequent phase. This effort is focused on the Defense Industrial Base only. DoD is committed to working with the Department of Homeland Security to assess how the model designed for the DIB Pilot might apply to other sectors of the nation's critical infrastructure.

6.1 (U) Breadth of Coverage

(U//~~FOUO~~) In follow-on phases the assumption is that more time will allow the other Tier 1 ISPs, as well as other non-Tier 1 ISPs or security service providers, some of whom may be DIB companies themselves, to build the necessary technical capability required to support the protection of critical DIB network traffic in a manner similar to that of the Pilot. Furthermore, increasing participation will naturally facilitate the incorporation of additional DIB entities into the program. However, such increases within the DIB require careful consideration to ensure that any solution remains scalable, particularly with respect to the protection of sensitive DoD equities, and within the scope of current DoD authorities.

6.2 (U) Depth of Capability

(U//~~FOUO~~) The extent of the network defensive capability chosen for the Pilot was also significantly limited by the critical desire to implement and operate the Pilot in a relatively short time interval (60-90 days). Therefore, to accommodate this aggressive schedule, the DIB Pilot was limited to only (b)(3) P.L. 86-36. In order to increase the defense of DIB network traffic, subsequent phases to protect the DIB would certainly include the expansion of (b)(3) P.L. 86-36 scenarios. Furthermore, other possibilities for increased effectiveness in protecting DIB network traffic through Pilot expansion in follow-on phases involving the DIB could include things such as: (b)(3) P.L. 86-36

[redacted]

6.3 (U) Business Model

(U//~~FOUO~~) The Business Model developed for the DIB Pilot is exclusive to the Pilot phase, and will very likely not be implemented in later phases (assuming that the Pilot is successful and the DoD elects to move to sustained operational phases). Therefore, additional planning is necessary to determine the options for a Business Model for future phases involving the DIB or for DHS-lead expansion into other sectors. The Business Model will need to address which entity (i.e. DIB entity or USG) funds the hardware and software costs of the ISP's enhancement of their managed security services. The most appropriate business model is likely to be for the ISP's to charge protected entities (i.e. a DIB company) for the provision of enhanced security services.

(U//~~FOUO~~) Following the pilot, the Government will engage with the ISPs and DIBs for recommendations on the future business model.

Appendix A - (U) Participating ISP Companies

(U) The following ISP companies were down selected as part of the DIB Pilot planning effort and may participate in the DIB Pilot:

- AT&T
- (b)(4) and (b)(7) [redacted]
-

Appendix B - (U) Participating DIB Companies

(U) As noted above, (b) (7)(E) [redacted] Defense Industrial Base companies have either provided intent to participate or are considering participation in the DIB Pilot. A final list will be compiled within two weeks of approval of the Plan.

Appendix C - (U) DNS Sinkholing Data Elements

(U) From ISP to DIB

(U//~~FOUO~~) The ISPs have communicated their expectation to provide DIB companies, on a per incident basis, the following alert information obtained from the safe server communications:

- Date/time stamp
- Source & destination IP
- Source & destination Port
- Protocol
- Possibly other information as described below

(~~S~~// (b)(3) P.L. 86-36, (b)(1) [redacted]

(U//~~FOUO~~) (b)(3) P.L. 86-36, (b)(1) [redacted]

(U//~~FOUO~~) From ISP to USG

(U//~~FOUO~~) For the DNS Sinkholing scenario, the ISP will provide aggregated reports including the following information based on the safe server communications and domain list hits to the USG through DoD. DoD will forward the anonymized_information to DHS:

- DIB company name
- Date/time stamp for each incident
- Destination port for each incident
- Protocol for each incident

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

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

Appendix D - (U) Malicious Email Filtering Data Elements

(U) From ISP to DIB

(U//~~FOUO~~) For the Malicious Email Filtering scenario, the ISP is expected to provide, on a per incident basis, the following alert information:

- Date/time stamp
- Email address information (From/To/CC)
- Email subject
- Name(s) of any attachment(s)
- Size(s) of any attachment(s)
- Malicious email (through a secure mechanism determined by the ISP)

(U//~~FOUO~~) From ISP to USG

(U//~~FOUO~~) For the Malicious Email Filtering scenario, the ISP will provide aggregated reports including the following information to the USG (through DoD, who will forward anonymized information to DHS):

- DIB company name
- Date/time stamp
- Type(s) of any attachment(s)
- (b)(3) P.L. 86-36, (b)(1)
- (b)(3) P.L. 86-36, (b)(1)

Note: Only the infected DIB entity will receive the Email Address information and Malicious Email. The USG will not receive this information.

Appendix E – (U) Abbreviations and Acronyms

ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
CAIDA	Cooperative Association for Internet Data Analysis
COA	Course of Action
CS	Cyber Security
DC3	Department of Defense Cyber Crime Center
DCFL	Defense Cyber Crime Center's Computer Forensics Lab
DFARS	Defense Federal Acquisition Requlation Supplement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DNS	Domain Name Service
DoD	Department of Defense
DSD	Deputy Secretary of Defense
E3	EINSTEIN 3
FA	Framework Agreement
IA	Information Assurance
IP	Internet Protocol
ISP	Internet Service Provider
MAC	Mandatory Access Controls
MOU	Memorandum of Understanding
NIPRNet	Non-classified Internet Protocol Router Network
NSA	National Security Agency
SCIF	Sensitive Compartmented Information Facility
SLA	Service Level Agreement
TEM	Technical Exchange Meeting
TTP	techniques, tactics, and procedures
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USG	United States Government
USTRANSCOM	United States Transportation Command

Appendix F – (U) Legal Annex to DIB Pilot Cybersecurity Plan

I. (U) DoD Authorities and Responsibilities

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