NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 78711A
12 March 2015

ALAN BUTLER
EPIC
1718 CONNETICUT AVE NW STE 200
WASHINGTON DC 20009

Dear Mr. Butler:

This is an interim response to your Freedom of Information Act (FOIA) request of 1 August 2014, which was received by this office on 1 August 2014, for the following:

1) "Any policies, regulations, white papers, final memoranda, guidelines, or training materials interpreting or addressing the collection, retention, dissemination, or sharing of electronic communications or metadata under EO 12333.

2) The most recent version of IC member agency procedures adopted under EO 12333, including DOD 5240 1-R, Army Regulation 381-10, and USSID-18."

As previously informed, your request has been assigned Case Number 78711. This letter indicates that we have begun to process your request. In our letter dated 6 August 2014, we also informed you that for purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. As such, you are entitled to free search and 100 pages of duplication. Since there are no assessable fees associated with your request, we did not address your request for a fee waiver.

We have completed the search for responsive material. One of the documents responsive to your request has been located in a prior FOIA request, Case 78117, which is in a backlog awaiting review. We will provide an interim response to you when processing of the material in this prior FOIA has been completed.

Additionally, we have located one other record responsive to your request that requires review prior to release and has been placed in the first-in, first-out processing backlog queue. Please be advised that there are a significant number of cases ahead of yours in the queue. We appreciate your patience with our efforts to treat all requesters fairly by responding to each on a "first-in, first-out" basis. We will respond to you when processing of the materials responsive to your request has been completed.

Furthermore, we have located another document (enclosed with this letter) that was previously released in a similar FOIA case, which we feel is also responsive to your request.

Finally, there is a wealth of information that has been made available to the public, which is responsive to the information you seek. You can locate that information on the following three Internet web sites; www.nsa.gov, www.dni.gov, and www.IContherecord.tumblr.com. As a courtesy, we have identified seventeen documents that are responsive to your request that have been posted to two of these web sites as follows:

- "National Security Council Intelligence Directive 6 (NSCID-6), " dated, 17 February 1972, www.nsa.gov web site.

Note: The following documents have been posted to the www.IContherecord.tumblr.com web site and can either be found directly on the home page or under the "Declassified Documents" heading.

- "National Security Agency Central Security Service NSA/CSS Policy 1-23, Procedures Governing NSA/CSS Activities that Affect U.S. Persons," dated 11 March 2004

- "Department of Defense, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons (DoD 5240 1-R)," dated December 1982

- "United States Signals Intelligence Directive 18 (USSID 18)," dated 27 July 1998

- "United States Signals Intelligence Directive 'USSID 18 Annex J,' Procedures for Monitoring Radio Communications of Suspected International Narcotics Traffickers," dated 24 April 1986

- "United States Signals Intelligence Directive USSID SP0018, Legal Compliance and U.S. Persons Minimization Procedures," dated 25 January 2011

- "NSA Cryptologic School Course on Legal, Compliance, and Minimization Procedures," dated August 2009.

- "Department of Defense Supplemental Procedures of Communications Metadata Analysis (SPCMA)," dated 3 January 2008 (released 11 September 2014)

- "Dissemination of US Person Information Among Elements of the US Intelligence Community," dated 23 June 2010

- "Sharing of 'Raw SIGINT' through Database Access," dated 12 July 2007

- "Legal Fact Sheet: Executive Order 12333," dated 19 June 2013

- "SID Management Directive Number 421, United States SIGINT System Database Access," dated 30 April 2007

- "SID Management Directive Number 422, United States SIGINT System Mission Delegation," dated 30 April 2007

- "SID Management Directive Number 432, Procedural Guidelines for SIGINT Production on U.S. [redacted] Field Exercises," dated 5 May 2010

- "Overview of Signals Intelligence Authorities (OVSC1100)," dated 8 January 2007

- "United States Signals Intelligence Directive (USSID SP0019), NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy," dated 13 November 2012

- "United States Signals Intelligence Directive, 'SIGINT Production and Raw SIGINT Access' (USSID CR1610)," dated 25 August 2005

Any correspondence related to your request should include the case number assigned to your request. Your letter should be addressed to

National Security Agency, FOIA Office (DJ4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

CStacker FOR

PAUL J. BLASKOWSKI
Chief
FOIA/PA Office

Encl:
a/s

SIGNALS INTELLIGENCE DIRECTORATE
SID MANAGEMENT DIRECTIVE NUMBER 424
Issue Date: 29 November 2010
Revised Date: 8 November 2012
POC: SIGINT Development Strategy and Governance (SSG), and SID Oversight and Compliance (SV)

(U//~~FOUO~~) SIGINT DEVELOPMENT - COMMUNICATIONS METADATA ANALYSIS

(U) Purpose

~~(S//SI//REL)~~ In accordance with NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," this Signals Intelligence Directorate (SID) Management Directive (SMD) provides guidance on the National Security Agency/Central Security Service (NSA/CSS) implementation of the "Department of Defense Supplemental Procedures Governing Communications Metadata Analysis" (SPCMA) as approved by the U.S. Attorney General for communications metadata collected under Executive Order 12333, as amended, authorities. It additionally addresses the implementation of similar processes and procedures for data collected under specific Foreign Intelligence Surveillance Act of 1978 (FISA) authorities when such processes and procedures are authorized. See Annex B for guidance specific to data collected pursuant to FISA authorizations.

NOTE: (U) Underlined terms are defined in the Definitions section.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20370501~~

(U) Scope

~~(S//SI//REL)~~ This SMD applies to any SID organization or Extended Enterprise U.S. SIGINT System (USSS) element that is authorized to perform communications metadata analysis. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

~~(C//REL)~~ This SMD applies to all SIGINT processing and analysis systems that implement contact chaining [redacted] to communications metadata. Systems complying with this SMD are authorized [redacted] provided they demonstrably implement the internal controls required by this SMD and associated [redacted] requirements [redacted] Section II, „Policy", outlines the internal controls required by this SMD.

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

~~(U//FOUO)~~ [redacted] This SMD applies to the processing and analysis of communications metadata as defined in the Definitions section and does not affect the processing of content or other data collected by NSA/CSS. Furthermore, this SMD does not apply to collection, retention, or dissemination activities.

//S//
TERESA H. SHEA
Director
Signals Intelligence Director

DISTRIBUTION:
Signals Intelligence Directorate (all organizations)
SIGINT Enterprise, Field, (all organizations)
Office of General Counsel
Office of Policy & Records
Technology Directorate

I. (U) BACKGROUND

(U) Background

1. ~~(S//SI//REL)~~ [redacted] analysis of communications metadata, these efforts have been constrained by the application of rules written for processing the content of communications. These rules required that SIGINT analysts stop contact chaining [redacted] As a result, analysts frequently ceased chaining when they encountered [redacted] This increasingly hampered analysis of data already lawfully collected under NSA/CSS authorities. Consequently, NSA/CSS sought approval for a new set of rules that were more appropriate for processing communications metadata and that recognized that the legal standards governing communications metadata are quite different from those governing the contents of a communication.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

2. ~~(S//SI//REL)~~ In January 2008, the U.S. Attorney General approved the SPCMA, a supplement to DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," and the classified annex to DoD 5240.1-R. These supplemental procedures allow SIGINT analysts to perform communications metadata analysis, such as contact chaining, for valid FI purposes. [redacted] The conditions under which the use of such procedures is permissible are outlined below.

3. ~~(S//SI//REL)~~ The SPCMA governs USSS analytic use of lawfully collected communications metadata, and it does not authorize collection of additional data, nor does it authorize any changes in existing minimization procedures associated with data retention or the dissemination of SIGINT products or services.

> **NOTE:** (U//~~FOUO~~) The analysis of SIGINT collection that is regulated by FISA must be performed in accordance with pertinent minimization procedures governing that authorization (see Annex B). In order to support minimization decisions, the communications metadata will be labeled with the applicable collection authority and that data labeling will be available as a visual key to analysts, who are fully responsible for minimization.

II. (U) POLICY

(U) Process

4. ~~(S//SI//REL)~~ USSS personnel with a valid and documented FI purpose may employ complete contact chain analysis of communications metadata [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i
(b)(3)-18 USC 798

5. ~~(S//SI//REL)~~ Only USSS personnel who are working under the authority of the Director, NSA/ Chief, CSS (DIRNSA/CHSS), and who have a need for this data in the performance of their official duties will be authorized to use this capability to chain [redacted] collected communications metadata for FI purposes only.

[redacted]

NOTE: (U/~~FOUO~~) [redacted]

[redacted]

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

6. ~~(S//SI//REL)~~ The SPCMA sets forth three procedures for its use, as follows:

a. (U//~~FOUO~~) Communications metadata analysis will only be done for foreign intelligence purposes;

b. (U//~~FOUO~~) Results of the analysis will be disseminated in accordance with the appropriate minimization procedures; and

c. (U//~~FOUO~~) Any apparent misuse or improper dissemination will be investigated and reported.

7. (U//~~FOUO~~) This policy does not change existing authorities related to collection of communications metadata.

8. (U//~~FOUO)~~This policy does not change existing minimization procedures or policies associated with retention or dissemination of SIGINT data or information. Collection, retention, and dissemination activities must be conducted pursuant to the appropriate collection authority and minimization procedures.

9. (U//~~FOUO)~~For the purpose of applying these procedures, each initial (seed) query will require the analyst to enter an FI justification. The FI justification will apply to all traffic analysis performed as a result of the seed query. [redacted]

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

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

10. ~~(S//SI//REL)~~ [redacted]

11. (U//~~FOUO)~~ Recording FI justifications is intended to assist NSA/CSS analysts in memorializing the purpose of their communications metadata analysis activities. The FI justification documents the analytic knowledge linking the selector to a foreign target or foreign intelligence purpose. The FI justification is a memory aid in the event that the analytic process is questioned long after the fact. The justification preserves the rationale behind the query. FI justifications are subject to review (spot check).

(U) Training

12. ~~(C//REL)~~ Prior to being granted access to systems that support the SPCMA capability, personnel must complete the Office of General Counsel (OGC) and SID Oversight and Compliance (SV) approved training, and acknowledge an understanding of the rules governing the proper use of the data bases and chaining tools. Training will highlight the sensitivity of the data, the user"s obligations when accessing the data, the restriction on use of the data for FI purposes only, and the requirement to follow required dissemination procedures.

[redacted]

(b)(3)-P.L. 8

(U) Oversight

13. (U//~~FOUO)~~ USSS personnel must report any USSID SP0018, "Legal Compliance and Minimization Procedures," incidents to the Intelligence Oversight Officer (IOO), SV, NSA/CSS Inspector General (IG), and OGC for inclusion in existing or future compliance reporting mechanisms relating to NSA/CSS SIGINT activities. Incidents must be reported immediately upon recognition, and in the IO Quarterly Report. Non-compliant activity may result in corrective actions, to include account removal, retraining, or other actions as appropriate.

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

(U//~~FOUO~~) [redacted]

14. ~~(S//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(U) Special Processing

15. ~~(S//SI//REL)~~ [redacted]

III. (U) RESPONSIBILITIES

(U) OGC

16. (U//~~FOUO~~) NSA/CSS OGC has received and adjudicated those collected communications data fields that are appropriate for analysis as communications metadata within the context of this directive. [redacted]

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

[1] ~~(S//SI//REL)~~ [redacted]

[2] ~~(S//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

[redacted]

(U//~~FOUO~~)
17. ~~(S//SI//REL)~~ [redacted]

[redacted]

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

(U) SIGINT Development Strategy and Governance (SSG)

18. (U//~~FOUO~~) [redacted]

[redacted]

19. ~~(S//SI//REL)~~ [redacted]

[redacted]

(U) Data Stewards

20. ~~(S//SI//REL)~~ Data stewards (e.g., system managers/developers) will modify select SIGINT [redacted] systems to adhere to the requirements outlined below prior to implementation of SPCMA in a system. Data stewards will contact the Technology Directorate"s Office of Compliance (TV) for specific SPCMA technical requirements, and will follow corporate governance processes for SPCMA approval prior to deployment of SPCMA capability. Basic SPCMA requirements are outlined as follows:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

a. ~~(S//SI//REL)~~ [redacted]

[redacted]

b. (U//~~FOUO~~) Tools and capabilities must limit access to only those users who have successfully completed the mandatory training and are authorized to operate under the procedures.

c. (U//~~FOUO~~) Data stewards will modify tools to require the user to enter a FI justification as a normal part of the user mechanism initiating each user-generated query or workflow for contact chaining. Software may provide accelerators to make this as easy as possible, but the accelerator will not be populated with canned default justification statements.

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

d. (U//~~FOUO~~) Data stewards will implement a help function with appropriate information [redacted] All such help displays will be vetted through OGC and SV.

e. (U//~~FOUO~~) Tools will log all user-generated queries. At a minimum, log entries will include: user-id; user-organization; date/time group; query or workflow, and FI justification. These logs will be stored in the appropriate standard corporate database [redacted]

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

f. ~~(S//SI//REL)~~ All applications [redacted] complying with the conditions of this SMD (i.e., those applications through which the unminimized data can be accessed) will display a banner that emphasizes the mandatory instructions regarding use of the unminimized data and chaining tools, and instructions for proper retention and dissemination of any results obtained. Users who do not positively acknowledge the banner will not have access to SPCMA-enabled accounts. The banner will display the following text when the application is launched:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

> ~~(S//SI//REL)~~ *This is a raw SIGINT system. The data contained is not evaluated for foreign intelligence,* [redacted] *All queries against this data must be conducted for a foreign intelligence purpose.* [redacted] *Queries may require additional justification and may be subject to additional intelligence oversight procedures. Records of all queries will be retained for intelligence oversight and compliance purposes. By acknowledging, I accept responsibility and remain accountable for the compliance of any ensuing queries.*

(U) Mission Supervisors

21. (U//~~FOUO~~) Mission supervisors will validate the mission need, based on the mission description, when users apply for accounts to systems that comply with the conditions of

this directive. Mission supervisors will spot check analyst activities in the database to ensure that they remain compliant with the SPCMA-defined procedures.

22. (U//~~FOUO~~) Spot checking communications metadata queries differs from active or passive auditing of content queries. Spot checking focuses on activity that has an increased likelihood of being improper, unauthorized, or questionable with respect to legal compliance or minimization procedures. Therefore, the minimum standards for spot checking communications metadata queries are:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

a. ~~(S//REL)~~ [redacted] of all queries run by the collection of assigned analysts will be reviewed within seven (7) days of query; and

b. ~~(S//REL)~~ [redacted] of all queries run by the collection of assigned analysts will be reviewed within seven (7) days of query.

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

NOTE: (U//~~FOUO~~) [redacted] Mission elements may choose to implement higher standards at their discretion.

(U) Analysts

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

23. ~~(S//SI//REL)~~ [redacted] Analysts using SPCMA-enabled tools are responsible for following the applicable minimization procedures. Therefore, analysts will complete mandatory training approved by the NSA/CSS OGC and SV prior to using a SPCMA-enabled tool. The minimum training requirements are OVSC1000, OVSC1100, OVSC1800, and the SPCMA read-on. Mandatory training is tracked in [redacted] and validated for access in [redacted] Also, during this process the user will acknowledge understanding of and accept responsibility for the proper use of communications metadata databases and chaining tools prior to obtaining access to and using a SPCMA-enabled tool.

24. ~~(C//REL)~~ Analysts will enter an FI Justification [redacted] to initiate communications metadata analysis, to include a query or workflow that generates contact chains.

25. (U//~~FOUO~~) Analysts will continue to follow minimization procedures appropriate to the collection authority of the underlying data when retaining or disseminating the results of their analysis. Since the communications metadata will be appropriately labeled with collection authority, that data labeling will be available as a visual key to guide retention and dissemination decisions.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

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

(U) SV

26. (U//~~FOUO~~) SV is responsible for the oversight standards and compliance verification procedures necessary to ensure proper adherence to the requirements governing this activity. This includes verifying compliance, requiring spot checks, and following through with associated incident reporting. SV may conduct periodic super audits of activities related to the SPCMA to verify that activities remain properly controlled.

IV. (U) DEFINITIONS

(U) Accelerators

27. (U//~~FOUO~~) Accelerators provide the capability to retain query histories in a menu format for reuse.

(U) Communications Metadata

28. ~~(S//SI//REL)~~ The dialing, routing, addressing, or signaling information associated with an electronic communication event. Communications metadata does not include information concerning the substance, implication, or meaning of the communication. [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(U) Contact Chaining

29. ~~(S//REL)~~ The linking and analysis of multiple communications addresses to discover relationships between communicants [redacted]

(U) Dialed Number Recognition

30. ~~(S//SI//REL)~~ [redacted]

(U) Digital Network Intelligence (DNI)

31. ~~(S//REL)~~ [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

[redacted]

(U) Super Audit 32. (U//~~FOUO~~) A super audit is a high-level review of queries made against NSA/CSS raw SIGINT databases. These compliance checks will be performed randomly across the full user base of SIGINT systems.

(U) U.S. Person 33. (U) A citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. (From the Foreign Intelligence Surveillance Act of 1978). See U.S. Signals Intelligence Directive SP0018 for additional information.

(U) WaveLegal 34. (U) NSA/CSS auditing tool.

(U) Workflow 35. (U//~~FOUO~~) Any follow-on processes once an initial query is run.

V. (U) REFERENCES

(U) References 36. (U) NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," revised 29 May 2009.

37. ~~(S//SI//REL)~~ FISA Amendments Act (FAA) 702 Oversight Procedures, [redacted] December 2011.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

38. ~~(S//SI//REL)~~ Department of Defense Supplemental Procedures Governing Communications Metadata Analysis, 2008.

39. (U) Executive Order 12333, "United States Intelligence Activities," as amended in 2008.

40. (U) Foreign Intelligence Surveillance Act of 1978.

41. (U) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD

Intelligence Components that Affect United States Persons," December 1982.

42. (U) "Classified Annex to Department of Defense Procedures Under Executive Order 12333," 27 May 1988

43. (U//~~FOUO~~) U.S. Signals Intelligence Directive SP0018, "Legal Compliance and Minimization Procedures." 27 July 1993.

ANNEX A

~~(S//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-50 USC 3024(i
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

ANNEX B

~~(S//SI//REL)~~ ANALYSIS OF METADATA COLLECTED PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

(U) Introduction

1. ~~(S//SI//REL)~~ The following guidance is provided to aid analysts who are involved in analyzing communications metadata collected pursuant to the Foreign Intelligence Surveillance Act (FISA).

(U) Policy on Metadata Analysis

2. ~~(TS//SI//REL)~~ The minimization procedures described below have been approved by NSA/CSS Office of General Counsel (OGC) and have been determined by NSA/CSS OGC to authorize processing of metadata pursuant to the Supplemental Procedures Governing Communications Metadata Analysis (SPCMA) as described in the main body of this SID Management Directive (SMD). [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

NSA/CSS analysts may chain [redacted] and perform similar metadata analysis on such data. [redacted] as long as the analysts have a valid foreign intelligence purpose. Analysts must adhere to the requirements set forth in the respective minimization procedures with regard to retention and dissemination:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

- ~~(S//SI//REL)~~ [redacted]
- ~~(S//REL)~~ [redacted]

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

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]

NOTE: ~~(TS//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

- (U//~~FOUO~~) [redacted]

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

3. (U//~~FOUO~~) Additionally, the data must be labeled in a manner that clearly identifies that which was obtained pursuant to each type of FISA authorization. FISA-labeled data must only be made available to personnel who have received training in the relevant FISA minimization procedures.

(U) Dissemin-ation

4. ~~(S//SI//REL)~~ Dissemination of U.S. person information that comes from communications metadata analysis is governed by the pertinent minimization procedures under which the data was originally acquired. Before an analyst disseminates information that comes from communications metadata analysis and that

identifies a known or presumed U.S. person [redacted] the analyst shall ensure that it meets the standards in the minimization procedures under which the data was originally acquired.

(U) Potential Changes to FISA Minimization Procedures

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

5. ~~(S//SI//REL)~~ [redacted] [redacted]

6. ~~(S//SI//REL)~~ Any questions concerning the processing of metadata derived from authorizations pursuant to FISA should be directed to the OGC Intelligence Law Practice Group.

ANNEX C

(U//~~FOUO~~) [redacted] [redacted]

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

(U//~~FOUO~~) [redacted] [redacted]

(U//~~FOUO~~) [redacted] [redacted]

(U//~~FOUO~~) [redacted] [redacted]

~~(S//SI//REL)~~ [redacted]

- [redacted]
-

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

- [redacted]
  - [redacted]

[redacted]

(U/~~FOUO~~) [redacted]

[redacted]

(U/~~FOUO~~) [redacted]

[redacted]

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