~~TOP SECRET//SI//NOFORN~~

STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
RODNEY PATTON
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460

Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.* Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.* Defendants.	No. 08-cv-4373-JSW
FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 13-cv-3287-JSW **CLASSIFIED DECLARATION OF TERESA H. SHEA** ***EX PARTE, IN CAMERA* SUBMISSION** Date: March 19, 2014 Time: 2:00 P.M. Courtroom: 11 – 19th Floor Judge Jeffrey S. White

I, Teresa H. Shea, do hereby state and declare as follows:

(U) INTRODUCTION

1. (U) I am the Director of the Signals Intelligence Directorate (SID) at the National Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for the collection, processing, and dissemination of Signals Intelligence information for foreign intelligence purposes of the United States. I have been designated an original TOP SECRET classification authority under Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Directive No. 5200.1-R, Information Security Program (Feb. 24, 2012).

2. (U) My statements herein are based upon my personal knowledge of Signals Intelligence collection and NSA operations, information available to me in my capacity as Signals Intelligence Director, and the advice of counsel.

3. (U) This declaration is classified TOP SECRET//SI//NOFORN pursuant to the standards in Executive Order 13526, 3 C.F.R. 298 (2009). Under Executive Order 13526, information is classified "TOP SECRET" if disclosure of the information reasonably could be expected to cause exceptionally grave damage to national security, "SECRET" if disclosure of the information reasonably could be expected to cause serious damage to national security, and "CONFIDENTIAL" if disclosure of the information reasonably could be expected to cause identifiable damage. In addition to classified information, this declaration also references Special Intelligence (SI), which is a subcategory of Sensitive Compartmented Information (SCI), for which the Director of National Intelligence (DNI) imposes additional safeguards and access requirements. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the degree of sensitivity of the information contained in the paragraph.

4. (U) When used for this purpose, letters "U," "C," "S," and "TS" indicate, that the information is UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET,

respectively. Where "SI" information is at issue in the paragraph, these letters will follow after the classification letters.

5. (U) Finally, and in addition to the separate levels of classification markings defined by Exec. Order 13526, there are also dissemination controls appropriately associated with classified information. Dissemination control markings identify the expansion or limitation on the distribution of the information. Not Releasable to Foreign Nationals, indicated by the abbreviation NOFORN or NF, is an explicit foreign release marking used to indicate that the information may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator of the information.

6. (U) Accordingly, none of the information in this declaration can be removed from classified channels without prior review by NSA and cannot appear in the public record, including the docket reflecting these proceedings.

(U) DESTRUCTION OF COLLECTED TELEPHONY METADATA IN COMPLIANCE WITH FISC MINIMIZATION REQUIREMENTS

7. (U) Under the "business records" provision of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1861, as enacted by section 215 of the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("Section 215"), the Foreign Intelligence Surveillance Court ("FISC"), upon application by the Federal Bureau of Investigation (FBI), may issue an order "for the production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism." 50 U.S.C. § 1861(a)(1). Since May 2006, the NSA has collected bulk telephony metadata ("data") pursuant to FISC orders directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of "call detail" records[1] created by the recipient providers for calls to, from, or wholly within the United States. Under the FISC's orders, the NSA's authority to continue collecting the data expires after approximately 90 days and must be renewed. The FISC has

[1] ~~(TS//SI//NF)~~ Under the terms of the FISC's orders, this data includes, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call.

renewed the daily collection of these data approximately every 90 days since May 2006 based on applications from the FBI, supported by the NSA, showing that the production of these call detail records satisfies the requirements of Section 215. To protect U.S. person information the FISC's orders impose procedures to minimize access to, use, dissemination, and retention of the data consistent with the need to acquire, produce, and disseminate foreign intelligence information. Among these is the requirement to destroy all bulk telephony metadata obtained under the FISC's Section 215 orders within five years (60 months) of the data's collection. This five-year limit reflects the judgment arrived at by the Executive Branch that after five years the data no longer holds significant foreign intelligence value meriting their retention.

8. ~~(TS//SI//NF)~~ The NSA effectuates this retention limit using existing computer systems architecture (referred to herein as the "existing architecture") by implementing [redacted] compliance process during which the NSA destroys the data to be aged off [redacted] beforehand. Thus, at any given time the NSA has [redacted] worth of data, but not more than five years. [redacted] NSA intelligence analysts do not and will not have access to any data that

are otherwise subject to the FISC-imposed destruction requirement while the question of whether the data must be preserved for litigation purposes is being resolved. Nor would they have access to the data afterward if they are preserved.[2]

9. ~~(TS//SI//NF)~~ The NSA has for several years been in the process of developing a new computer systems architecture (referred to herein as the "new architecture") for storing and processing the telephony metadata collected pursuant to the FISC's orders under Section 215. The purpose of this new architecture is to better ensure compatibility with NSA-wide information technology upgrades. [redacted]

[redacted]

10. (U) I have been informed that Plaintiffs in these actions have requested that the Government be required to preserve the "telephone records" that the NSA has collected under the FISC-authorized telephony metadata program. This request could be taken to mean either (i) targeted preservation of metadata collected under Section 215 that pertain only to the

[2] (U) By order of the FISC on March 12, 2014, NSA technical personnel may access the metadata only for the purpose of ensuring continued compliance with the Government's preservation obligations to include taking reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued integrity of the BR metadata.

Plaintiffs' telephone calls, if any, or (ii) mass retention of all the data that are more than five years old. Both tasks would impose significant financial burdens on the NSA, divert personnel and technological resources from performance of the NSA's national security mission, and present other issues as well. I discuss each task in turn.

(U) CONTINUED RETENTION OF COLLECTED TELEPHONY METADATA, IF ANY, RELATED TO PLAINTIFFS' TELEPHONE CALLS

11. ~~(TS//SI//NF)~~ To the extent Plaintiffs seek targeted preservation of data associated only with their own telephone calls, the NSA first would have to determine whether it has ever collected data pursuant to Section 215 associated with Plaintiffs' calls. For the NSA to make this determination, each Plaintiff organization and each individual Plaintiff would have to provide the NSA with, for example, all telephone numbers they were assigned or used at any time during the period for which data that otherwise would be destroyed must be preserved [redacted] The Plaintiffs would also have to inform the NSA of the specific time period during which they were assigned or used each telephone number, so that data pertaining to the calls of other persons who may have used or been assigned a particular number are not inadvertently retained. For the same reason, if this litigation continues long enough, each Plaintiff would have to inform the Government of any changes in the numbers they use or are assigned.

12. (U) It is also important to note that the NSA would not simply be preserving data consisting of the Plaintiffs' phone numbers; the preserved data would include, among other information, the initiating and receiving number, and the date, time, and duration of each call in each record that was collected. For example, if a call detail record concerning a phone call made by a Plaintiff was collected, that Plaintiff's telephone number as well as the receiving number—which may be that of an individual not in any way associated with these lawsuits—would be preserved together, along with the date, time, and duration of that individual's call with the Plaintiff.

13. (U) Moreover, pursuant to the FISC's orders, NSA intelligence analysts may not access the data except through queries conducted for foreign intelligence purposes using

identifiers (e.g., telephone numbers) that are reasonably suspected of being associated with foreign terrorist organizations that have been approved for targeting by the FISC. Therefore, even if Plaintiffs were to provide the NSA with the telephone numbers they used or were assigned during the relevant time period, to identify records of Plaintiffs' calls would possibly require prohibited queries of the database for purposes other than obtaining foreign intelligence information by using identifiers (Plaintiffs' telephone numbers) that have not been approved under the "reasonable, articulable suspicion" standard. This means that, before determining whether the NSA has collected metadata associated with Plaintiffs' calls, the Government may first have to seek and obtain approval from the FISC to run queries in the NSA's database for records associated with each telephone number provided by each Plaintiff. In the event that data associated with any calls made by Plaintiffs have been collected by the NSA, the queries, among other things, will return—and, in accordance with any preservation obligation imposed by the Court, the NSA would separately maintain—a collection of records indicating the telephone numbers with which each Plaintiff was in contact over a period of one or more years, depending on how long the NSA must continue to preserve data it would otherwise destroy.

14. (U) In addition to the foregoing considerations are the time, effort, and resources that would be required for the NSA to preserve until the conclusion of the litigation any data (whether pertaining to Plaintiffs' calls only or not) that would otherwise have been destroyed in compliance with the FISC's five-year retention limit. The fact that there is no way to predict how long the lawsuits before this Court will last, coupled with ever-changing mission requirements and systems, makes it extremely difficult to estimate costs and to devise the most cost-effective data storage solution should this Court issue an order requiring preservation of data that would otherwise be subject to age-off. All of the feasible solutions present the possibility of imposing substantial cost burdens on the NSA that would divert limited resources away from foreign intelligence mission requirements. While it is impossible to quantify the additional risks such a diversion of resources may pose to the national security, I deem such risks to be significant.

15. (U) An order to preserve only metadata pertaining to Plaintiffs' calls (assuming such

data have been collected) would require the NSA to devote significant financial and personnel resources over several months—assets that would otherwise be devoted to the NSA's national security mission—to create, test, and implement a solution that would preserve only these targeted data on an ongoing basis.

16. ~~(TS//SI//NF)~~ Specifically, with regard to the new architecture, which is currently scheduled to replace the existing architecture later this year, the NSA would need to assign a team of NSA software developers, already familiar with the Section 215 telephony metadata program and the relevant platform, to create and design appropriate software and write the source code that would allow the NSA to identify and separately retain the telephony metadata associated only with Plaintiffs' telephone numbers, if any, that would otherwise be aged off and destroyed on a daily basis. Once the software had been created, this NSA team would need to test and verify that the program works as intended, resolve any flaws or bugs, and then (as with any significant modification to an existing architecture) seek and obtain approvals within the NSA for implementation of the new software program. I estimate, based on the information available to me now, that this process would take the team of NSA software developer [redacted] of full-time work on the project from deployment to operational capability. The cost of this process is difficult to quantify in the abstract, but I would estimate that the initial cost would be at least [redacted] Additional costs would accrue over time. Over the course of three years, I estimate the total cost, including for the aforementioned labor, hardware maintenance, back up media, and additional software maintenance, would be at least [redacted] Over five years, I estimate the total cost would be at leas[redacted]l emphasize that these are preliminary estimates. Additional time would be needed in order to develop more complete and accurate estimates. Based on past experience, I believe that costs could well exceed these estimates and the estimates that follow in subsequent paragraphs of my declaration. In addition to the inherent difficulty of finding sufficient funds in the NSA's budget to cover such unanticipated costs, mission-enhancing functions would be delayed or impaired while resources are diverted to the preservation effort. For example, the software developers needed for this effort would be unable to work on NSA mission requirements during this [redacted]

period, causing delay in making the new architecture operational.

17. ~~(TS//SI//NF)~~ Hiring contractors or assigning other software developers who are not familiar with the Section 215 program or the new architecture to resolve this issue is not a viable option. The platform for the new architecture is proprietary and was developed by the NSA for purposes of the Section 215 program. Without devoted personnel who are experienced with the platform and its software, this process would take [redacted] (instead of [redacted] to allow for the additional training to assure successful completion of the work.

18. ~~(TS//SI//NF)~~ With regard to the existing architecture, NSA would be required, in order to preserve any metadata associated with Plaintiffs' calls that may have been collected and stored in that platform, to create, design, and write a software program that would allow the NSA to query the data for records associated with Plaintiffs' telephone numbers. Once responsive data, if any, were identified, NSA would then need to extract that data from the analytic databases and store it separately in an appropriate format. I estimate that the initial costs for personnel time and hardware alone would be at least [redacted] Over three years, I estimate the total cost, including for personnel time and hardware, would be well in excess of [redacted] Over five years, I estimate the total cost would be at least [redacted] Again, I emphasize that these are preliminary estimates. Depending on when the transition to the new architecture occurs, additional costs to preserve data in the existing architecture and maintain some or all of the additional architecture may also accrue.

19. ~~(TS//SI//NF)~~ In sum, based on the foregoing, I estimate that, if the Court orders the Government to preserve metadata associated with Plaintiffs' calls, the initial cost would be [redacted] and at least approximately [redacted] Over three years, I estimate the total cost would be approximately [redacted] and possibly more. Over five years, I estimate the total cost would be well in excess of [redacted] These preliminary cost estimates are in monetary terms only and do not factor in the diversion of personnel and technological resources from the NSA's foreign intelligence mission.

~~TOP SECRET//SI//NOFORN~~

(U) RETENTION OF ALL "AGED OFF" TELEPHONY METADATA FOR THE DURATION OF THE LITIGATION

20. ~~(TS//SI//NF)~~ The alternative to identifying, extracting, and preserving metadata pertaining just to Plaintiffs' telephone calls would be to preserve all telephony metadata collected more than five years ago in a format that precludes any access or use by NSA personnel for any purpose other than ensuring continued compliance with the Government's preservation obligations (to include taking reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued integrity of the data.) [redacted]

21. ~~(TS//SI//NF)~~ As described below, all data retained beyond the five-year retention limit specified in the FISC's orders could be preserved either by (i) maintaining all the data, [redacted] on a non-analytic portion of the existing architecture's software and hardware, or (ii) by migrating the all the data to backup tapes. Under either option, preservation of all telephony metadata retained beyond the five-year limit imposed by the FISC would involve substantial costs to the agency, financial and otherwise, either to preserve or to access the data (for litigation purposes). The first method of preservation would involve more costs initially but fewer costs to make the data retrievable. The second method would involve fewer upfront costs, but it would be significantly more expensive to retrieve the data and make them searchable for litigation purposes should that become necessary.

22. ~~(TS//SI//NF)~~ Regardless of whether NSA preserves the data using the existing architecture or by migrating the data to backup tapes, there is no way to guarantee with absolute certainty that over the course of time, the integrity of the data will be preserved. As a general matter, the longer the time that electronic data must be preserved, the greater the risk that such

data—in spite of best efforts by NSA personnel—will become unusable for litigation or for any other purpose.

(U) Option One

23. ~~(TS//SI//NF)~~ The first of the two options for preserving all of the data would involve migrating the data into a preservation system to which NSA intelligence analysts would have no access for any purpose. Further, some portion of the existing architecture, instead of being decommissioned, as is now planned for [redacted] would remain in operation for the sole purpose of preserving the data for civil litigation purposes.

24. ~~(TS//SI//NF)~~ [redacted]

25. ~~(TS//SI//NF)~~ An important goal of the evolution from the existing architecture to the new architecture is to realize cost savings through [redacted] A significant portion of those savings will be lost if the existing architecture cannot be decommissioned, as planned, once the new architecture becomes operational.

26. ~~(TS//SI//NF)~~ For example, continued operation of the hardware on which the existing architecture is located will require the NSA to continue to devote space in which to house the hardware, as well as electrical power needed to operate and cool it. These are critical resources, all in great demand at NSA given the breadth of the agency's responsibilities for the acquisition, analysis, and dissemination of foreign intelligence information. Continuing to devote these resources to the operation of the existing architecture for litigation purposes will mean diverting them, in effect, from ongoing (or intended) signals intelligence operations with a corresponding impact on the NSA's ability to collect, process, analyze, and disseminate foreign intelligence information for purposes of national security. In addition, preservation of data in the

existing architecture would require a diversion of qualified personnel resources from other NSA operational missions to maintain and repair the hardware and ensure the continued integrity of the stored data. Over the next year, I estimate the cost of this undertaking in monetary terms alone to be [redacted] and in the range of up to or exceeding [redacted] I emphasize that this is a preliminary estimate and the actual expenses may vary substantially from this figure if the Court ordered this option.

(U) Option Two

27. ~~(TS//SI//NF)~~ An alternative to the preservation of telephony metadata within the existing architecture would be to migrate data acquired more than five years ago from online databases to offline storage on tape. Under this option, all data would be copied onto sets of tapes for offline storage. [redacted]

28. ~~(TS//SI//NF)~~ Preservation of the data once they have been transferred onto tapes would not involve a diversion of financial, technological, and personnel resources on the same scale as preserving the data on an active, repurposed system within the existing architecture. Nevertheless, the cost remains substantial. Once metadata have been transferred to offline storage, the tapes containing the data would have to be maintained under appropriate environmental conditions (temperature and humidity) to maintain the integrity of the media and the preserved data. The estimated cost of this method would be approximately [redacted] per year simply to store the data without ever retrieving it. I emphasize that this is a preliminary estimate and the actual expenses may vary substantially from this figure.

29. ~~(TS//SI//NF)~~ These costs would greatly increase if the NSA were required to retrieve these data for litigation purposes. To make the data preserved on tapes accessible for possible purpose of discovery in litigation (e.g., to search for records of calls to or from the Plaintiffs) at a later date, would require substantial time and effort and impose additional significant costs on the NSA. [redacted] I emphasize that this is a preliminary estimate and actual expenses may vary substantially from this figure. The larger the amount of data that is preserved over time, the greater will be the time for needed and cost to the agency of making the data accessible in this fashion. As with any type of tape storage, there is also a risk that the integrity of the data could be compromised through the passage of time, and that the data may not be retrievable or searchable if the existing architecture cannot be made functional again.

(U) PRESERVATION OF OTHER POTENTIAL EVIDENCE

30. (U) I understand that the Plaintiffs have inquired what steps the Government has taken to preserve telephony metadata, Internet metadata, and communications content collected by the NSA under authority of the President following the September 11, 2001, terrorist attacks, and thereafter under FISC authority pursuant to sections 402, 501, and 702 of FISA, as well as other documents and information pertaining to those activities. I address those matters below. Nothing stated herein, however, is intended to be, or should be construed as, an admission either (i) that documents and information pertaining to activities carried out under FISC authority, including the data collected, are relevant to the *Jewel* litigation (or its companion case, *Shubert v. Obama*), or (ii) that documents and information pertaining to the collection of Internet metadata and communications content under FISC authority pursuant to sections 402 and 702 of FISA, including the data collected, are relevant to the *First Unitarian* litigation.

31. (U) The steps taken by the Government to identify and to preserve documents and

information related to the particular intelligence activities authorized by the President in the wake of the September 11 attacks are described in the Government's Classified Supplemental Memorandum in Opposition to the Plaintiff's Motion for Order to Preserve Evidence, dated October 25, 2007, filed in the case styled *In re NSA Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW. The Government supported its Memorandum with the Classified *in Camera, Ex Parte* Declaration of [redacted] Deputy Chief of Staff for Operations and Support, Signals Intelligence Division, National Security Agency to apprise the Court of the preservation efforts that the Government had undertaken. A declassified version of the Government's memorandum and [redacted] declaration have been prepared for public filing in this litigation. As explained in [redacted] declaration the NSA had at that time preserved, and the NSA continues to preserve, among other things, certain Internet and telephony metadata collected and the content of certain communications intercepted, under Presidential authority, in connection with the NSA intelligence programs known collectively as the President's Surveillance Program.

32. (U) It is not feasible in the time available to respond to Plaintiffs' Opening Brief re: Evidence Preservation to describe in detail the various steps that the NSA has taken to preserve documents and information related to the bulk collection of Internet and telephony metadata, and the collection of communications content, under FISC authority pursuant to sections 402 and 702 of FISA. With respect, however, to the retention of the collected data themselves, I can advise the Court as follows.

33. ~~(TS//SI//NF)~~ As discussed above, the FISC's orders authorizing the NSA's bulk collection of telephony metadata under FISA section 501 (Section 215) require that metadata obtained by the NSA under this authority be destroyed no later than five years after their collection. To comply with this legal requirement, the NSA between [redacted] of 2011, destroyed all the metadata collected between May 2006 (the inception of the program under FISC authorization) [redacted] Between [redacted] of 2012, the NSA destroyed all the metadata collected between [redacted] 2007 [redacted] Between [redacted] of 2013, the NSA destroyed all the metadata collected between [redacted] 2008 [redacted] with the exception of the test data, collected between [redacted] 2009. In accordance

with the Court's March 10, 2014, order, and the subsequent March 12, 2014, order of the FISC, the scheduled destruction of the data collected between [redacted] 2009, [redacted] has been put on hold pending further order of this Court. Therefore, the NSA currently retains bulk telephony metadata collected under FISC authority between [redacted] 2009, [redacted] and such data between [redacted] 2009 and the present.

34. ~~(TS//SI//NF)~~ The NSA's collection of bulk Internet metadata transitioned to FISC authority under section 402 of FISA in July 2004. Until December 2009, these data were subject under the FISC's orders to a 4.5-year retention limit, after which, pursuant to a change in the FISC orders, these data could be retained for up to five years. In December 2011, the Government decided not to seek FISC reauthorization of the NSA's bulk collection of Internet metadata because the program had not met operational expectations. Because the NSA did not intend thereafter to use the Internet metadata it had retained for purposes of producing or disseminating foreign intelligence information, in keeping with the principle underlying the destruction requirements imposed by the FISC, the NSA destroyed the remaining bulk Internet metadata in December 2011.

35. ~~(TS//SI//NF)~~ Certain of the NSA's acquisition of telephone and Internet content under Presidential authorization similarly transitioned to FISC authority. Beginning on January 10, 2007, the FISC issued orders (known as the "Foreign Telephone and Email Order" and [redacted] authorizing the Government to conduct certain electronic surveillance activities that had been occurring under the authority of the President. Presidentially authorized surveillance activities expired shortly thereafter. The FISC orders authorizing the electronic surveillance required that communications acquired under those authorities be destroyed no later than five years after their collection. All NSA intelligence reports utilizing the content of communications intercepted under authority of these orders are preserved permanently.

36. ~~(TS//SI//NF)~~ In August 2007, Congress enacted the Protect America Act (PAA), which carved out of the FISA definition of "electronic surveillance" a surveillance directed at a person reasonably believed to be located outside the United States and authorized the Attorney General and the Director of National Intelligence to jointly authorize the acquisition of foreign

intelligence information concerning persons reasonably believed to be located outside the United States. The Foreign Telephone and E-mail Order was not renewed after the PAA was enacted. Pursuant to applicable minimization procedures, the NSA was only authorized to retain communications acquired pursuant to PAA certifications for five years. Subject to limited exceptions, communications identified as domestic communications were to be promptly destroyed. All NSA intelligence reports utilizing the content of communications intercepted under PAA authority are currently retained permanently. The PAA expired on February 16, 2008 and, on July 11, 2008, the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA) was signed into law.

37. (U) Section 702 of FISA, enacted by the FAA, created new statutory authority and procedures permitting the targeting of non-United States persons reasonably believed to be outside of the United States without individual FISC orders through directives issued to electronic communication service providers by the Director of National Intelligence and the Attorney General. Pursuant to the FISC-approved (and mandated) minimization procedures in effect from August 2008 until October 2011, the NSA was only authorized to retain raw, unminimized communications acquired pursuant to § 702 certifications for five years. Subject to limited exceptions, domestic communications were to be destroyed upon recognition.

38. (U) On October 3, 2011, the FISC found certain aspects of NSA's § 702 minimization procedures to be inconsistent with certain statutory and constitutional requirements, including the retention of certain information acquired by NSA. Accordingly, NSA corrected the deficiencies identified by the FISC which, on November 30, 2011, found the retention provisions of NSA's amended minimization procedures to comply with both § 702 and the Fourth Amendment. The current NSA § 702 minimization procedures, which are in effect today, authorize NSA to retain telephony and certain Internet communications no longer than five years from the expiration date of the certification authorizing the collection. With respect to the retention of Internet transactions acquired via NSA's "upstream" techniques, such information must also be destroyed within two years of the expiration of the certification unless a limited exception applies. Further, any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011 will be destroyed upon recognition. Foreign

communications of or concerning United States persons collected in the course of an acquisition authorized under § 702 may be retained pursuant to certain, specified exceptions. Finally, subject to limited exceptions, domestic communications acquired pursuant to FAA 702 are to be destroyed upon recognition. All NSA intelligence reports utilizing the content of intercepted communications obtained under § 702 are preserved permanently.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: March 17, 2014

Teresa H. Shea

Teresa H. Shea