EXHIBIT 19

Termination Procedures for National Security Letter Nondisclosure Requirement

I. References

a. Right to Financial Privacy Act (RFPA), 12 U.S.C. §§ 3401-3422.
b. Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681-1681x.
c. Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2712.
d. Domestic Investigations and Operations Guide, Federal Bureau of Investigation, 2015.
e. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

II. Introduction

The FBI is statutorily authorized to issue NSLs only in connection with investigations to protect against international terrorism or clandestine intelligence activities and to obtain one of only four types of basic records: (i) telephone subscriber information, toll records, and other non-content electronic communication transactional records, *see* 18 U.S.C. § 2709; (ii) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, and institutions at which a consumer has maintained an account), *see* 15 U.S.C. § 1681u; (iii) full credit reports, *see* 15 U.S.C. § 1681v; and (iv) financial records, *see* 12 U.S.C. § 3414. An NSL may issue for these records only if the information being sought is relevant to an investigation to protect against international terrorism or clandestine intelligence activities, except that NSLs may not be used to obtain a full credit report in counterintelligence investigations unless there is an international terrorism nexus.

The FBI may impose a nondisclosure requirement on the recipient of an NSL only after certification by the head of an authorized investigative agency, or an appropriate designee, that one of the statutory standards for nondisclosure is satisfied; that is, where there is good reason to believe disclosure may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person. *See, e.g.,* 18 U.S.C. § 2709(c). The nondisclosure requirement prohibits the recipient of an NSL from disclosing information protected by the nondisclosure requirement to anyone other than: (i) those persons to whom disclosure is necessary in order to comply with the request; (ii) an attorney in order to obtain legal advice or assistance regarding the request; or (iii) other persons as permitted by the head of the authorized investigative agency, or a designee, described in the respective statute.

An NSL may issue, and a nondisclosure requirement may be imposed, only after rigorous review and approval at a high level. With respect to the NSL itself, an agent must justify in writing why the NSL is needed, i.e., the agent must provide a detailed explanation of the predication for the investigation as well as the relevance of the information sought. That written explanation, as well as the proposed NSL itself and any associated nondisclosure requirement, must be reviewed and approved by the Supervisory Special Agent, Chief or Associate Division Counsel, Assistant Special Agent in Charge, and Special Agent in Charge, or the equivalent-level officials at FBI Headquarters (FBIHQ).

The procedures set forth below (the "NSL Procedures") govern the review of the nondisclosure requirement in NSLs and termination of the requirement when the facts no longer support nondisclosure. These NSL Procedures also ensure that such reviews are initiated at established points in the life cycle of an investigation, and that such reviews and determinations are documented in the FISA Management System (FISAMS) and the FBI's central recordkeeping system, and any successor systems.

These NSL Procedures recognize and incorporate by reference existing limits mandated by statute on the imposition of the nondisclosure requirement in NSLs. The agent or analyst, Supervisory Special Agent, Chief or Associate Division Counsel, Assistant Special Agent in Charge, and Special Agent in Charge must assess whether the facts no longer support the nondisclosure requirement included in an NSL. If the facts no longer support the nondisclosure requirement, the FBI will provide notice to the recipient of the NSL, or officer, employee, or agent thereof, as well as to any applicable court, as appropriate, when the nondisclosure requirement has been terminated.

III. Review Procedures

A. Timeframe for Review

Under these NSL Procedures, the nondisclosure requirement of an NSL shall terminate upon the closing of any investigation in which an NSL containing a nondisclosure provision was issued except where the FBI makes a determination that one of the existing statutory standards for nondisclosure is satisfied. The FBI also will review all NSL nondisclosure determinations on the three-year anniversary of the initiation of the full investigation and terminate nondisclosure at that time, unless the FBI determines that one of the statutory standards for nondisclosure is satisfied.[1] When, after the effective date of these procedures, an investigation closes and/or reaches the three-year anniversary of the initiation of the full investigation, the agent assigned to

---

[1] Among other things, the USA FREEDOM Act requires the FBI to "review at appropriate intervals" the nondisclosure requirement of an NSL to assess whether facts supporting nondisclosure continue to exist. In the legislative history accompanying the Act, Congress indicated that:

> [t]hese procedures are based upon nondisclosure reforms proposed by President Obama in January 2014. In remarks accompanying the issuance of PPD-28, President Obama directed the Attorney General 'to amend how we use National Security Letters so that [their] secrecy will not be indefinite, and will terminate within a fixed time unless the government demonstrates a real need for further secrecy.' In January 2015, as part of its Signals Intelligence Reform 2015 Anniversary Report, the Director of National Intelligence announced that: In response to the President's new direction, the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of 3 years after the opening of a fully predicated investigation or the investigation's close. Continued nondisclosure orders beyond this period are permitted only if a Special Agent in Charge or a Deputy Assistant Director determines that the statutory standards for nondisclosure continue to be satisfied and that the case agent has justified, in writing, why continued nondisclosure is appropriate.

H. Rep. No. 114-109 (2015) at 24-25.

the investigation will receive notification, automatically generated by FBI's case management system, indicating that a review is required of the continued need for nondisclosure for all NSLs issued in the case that included a nondisclosure requirement. Thus, for cases that close after the three-year anniversary of the full investigation, the NSLs that continue to have nondisclosure requirements will be reviewed on two separate occasions; cases that close before the three-year anniversary of the full investigation will be reviewed on one occasion. Moreover, NSL nondisclosure requirements will be reviewed only if they are associated with investigations that close and/or reach their three-year anniversary date on or after the effective date of these procedures.

B. Review Requirements

The assessment of the need for continued nondisclosure of an NSL is an individualized one; that is, each NSL issued in an investigation will need to be individually reviewed to determine if the facts no longer support nondisclosure under the statutory standard for imposing a nondisclosure requirement when an NSL is issued—i.e., where there is good reason to believe disclosure may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person. *See, e.g.,* 18 U.S.C. § 2709(c). This assessment must be based on current facts and circumstances, although agents may rely on the same reasons used to impose a nondisclosure requirement at the time of the NSL's issuance where the current facts continue to support those reasons. If the facts no longer support the need for nondisclosure of an NSL, the nondisclosure requirement must be terminated.

Every determination to continue or terminate the nondisclosure requirement will be subject to the same review and approval process that NSLs containing a nondisclosure requirement are subject to at the time of their issuance. Thus, (i) the case agent will review the NSL, the original written justification for nondisclosure, and any investigative developments to determine whether nondisclosure should continue; (ii) the case agent will document the reason for continuing or terminating the nondisclosure requirement; (iii) the case agent's immediate supervisor will review and approve the case agent's written justification for continuing or terminating nondisclosure; (iv) an attorney—either the Chief Division Counsel or Associate Division Counsel in the relevant field office or an attorney with the National Security Law Branch at FBIHQ—will review and approve the case agent's written justification for continuing or terminating nondisclosure; (v) higher-level supervisors—either the Assistant Special Agent in Charge in the field or the Unit Chief or Section Chief at FBIHQ—will review and approve the case agent's written justification for continuing or terminating nondisclosure; and (vi) a Special Agent in Charge or a Deputy Assistant Director at FBIHQ will review and make the final determination regarding the case agent's written justification for continuing or terminating nondisclosure. In addition, those NSLs for which the nondisclosure requirement is being terminated will undergo an additional review at FBIHQ for consistency across field offices and programs. This review process must be completed within 30 days from the date of the review notice given by the FBI's case management system.

C. Notification of Termination

Upon a decision that nondisclosure of an NSL is no longer necessary, written notice will be given to the recipient of the NSL, or officer, employee, or agent thereof, as well as to any applicable court, as appropriate, that the nondisclosure requirement has been terminated and the information contained in the NSL may be disclosed. Any continuing restrictions on disclosure will be noted in the written notice. If such a termination notice is to be provided to a court, the FBI field office or FBIHQ Division that issued the NSL, in conjunction with FBI's Office of General Counsel, shall coordinate with the Department of Justice to ensure that notice concerning termination of the NSL nondisclosure requirement is provided to the court and any other appropriate parties.

D. Use of FBI Recordkeeping Systems

FBI will use its FISAMS system, or any successor system, to facilitate and document the review process described above. Once the decision to continue or terminate a nondisclosure requirement has been approved under the above review process, FISAMS will generate an electronic communication ("EC") that documents the justification and determination that will be serialized into the FBI's central recordkeeping system, unless otherwise exempted from being serialized. The FBI will also use FISAMS and its central recordkeeping system, and any successor systems, to facilitate the creation and transmittal of termination notices to NSL recipients and any court, as appropriate.

Audits to ensure compliance with these procedures will be included during the annual NSL reviews conducted by FBI's Inspection Division, as well as during periodic National Security Reviews conducted by the Department of Justice at each of FBI's 56 field offices.

E. Administrative Matters

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

The NSL Procedures will be effective 90 days from the date of the Attorney General's approval.

November 24, 2015

EXHIBIT 20

(U//FOUO) In addition to being signed by a statutorily-required approver, every NSL must be reviewed and approved by a CDC, ADC (or attorney acting in that capacity), or an NSLB attorney.

18.6.6.3.4 (U) Standards for Issuing NSLs

(U) The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is that the material sought is relevant to an authorized investigation to protect against international terrorism or clandestine activities, provided that such an investigation of an USPER is not predicated solely on activities protected by the First Amendment of the Constitution of the United States. Thus, an NSL may not be issued unless the information sought is relevant to an open and authorized Preliminary Investigation (PI) or Full Investigation (Full). **NSLs may not be issued in an Assessment. (An NSL request for a full credit report is not available in counterintelligence investigations unless there is an international terrorism nexus. 15 U.S.C. § 1681v.)**

(U//FOUO) Information is relevant if it tends to make a fact more or less probable. In the context of NSLs, there must be a reasonable belief that the information sought through the NSL either supports or weakens facts being investigated in an investigation. For example, financial records believed to support a subject's assertion that he or she was in the United States at a given time when the FBI believes he or she was outside the United States are relevant to the investigation because they tend to exculpate the subject. On the other hand, phone records of a sibling of a subject of an investigation not known to be in contact with the subject would not, barring additional information, be relevant to the national security investigation.

(U//FOUO) In addition to the information being relevant, the investigation of an USPER cannot be conducted solely based on activities protected by the First Amendment. For example, the FBI cannot issue an NSL for phone records of an individual solely because the individual attends a mosque that is also attended by international terrorism (IT) subjects. The individual's attendance at a place of worship is First Amendment-protected activity, on which the FBI cannot base an investigation. On the other hand, if the FBI reasonably believes that, in addition to attending the same mosque as the IT subjects, the individual received money transfers from IT subjects, then an NSL seeking his or her phone or bank records would be relevant to a national security investigation and would not be based solely on First Amendment-protected activities.

(U//FOUO) The EC that requests the issuance of an NSL must provide a sufficiently detailed explanation of the predication for the investigation and the relevance of the material sought by the NSL so that a meaningful review can be conducted. The information necessary to make a judgment regarding predication and relevance should be contained in the four corners of the EC. If the necessary information cannot be included in the EC because, for example, the information is classified Top Secret or the investigation involves insider espionage, the EC should clearly reference the source document that provides the predication and explain why the underlying information cannot be included in the EC.

(U//FOUO) Approval of an NSL must include a review of the predication of the underlying investigation. Although there is no legal review for opening an investigation, there must be a

review of the predicate for the investigation in determining whether an NSL request meets the legal standard of the relevant statutory authority.

(U//FOUO) As with all investigative methods, before requesting an NSL, the employee initiating the request should consider whether an NSL is the least intrusive and reasonable means based upon the circumstances of the investigation to obtain the needed information. See DIOG Section 4.4.

18.6.6.3.5 (U) Special Procedures for Requesting Communication Subscriber Information

(U//FOUO) If only subscriber information is needed for an investigation, an NSL should be issued for subscriber records rather than a broader request for subscriber and toll billing/transactional records.

(U//FOUO) Generally, all toll billing/transactional records responsive to the NSL may be uploaded into FBI databases. Before issuing NSLs seeking to identify a subscriber of facilities contained in such toll/transactional records, the employee should determine whether the identities of the subscribers of some or all of the telephone numbers/email accounts identified in the toll billing/transactional records are needed to advance the investigation. If so, the employee may issue subsequent NSLs to identify the subscriber(s) of such telephone numbers or email accounts. NSLs should not be used to identify the subscribers of numbers or email accounts if that information is not needed to advance the investigation and should not be issued unless and until that identity becomes needed for the investigation or some other investigation.

(U//FOUO) If a subscriber's identity may contribute to the investigation, the investigator should also consider whether an NSL is the least intrusive and reasonable means to obtain the information. In some instances, information obtained from open source or government databases may be sufficient to meet investigative needs. The information obtained from such sources may not be current or accurate; however, those factors, among others, should be considered in determining whether to issue an NSL.

18.6.6.3.6 (U) Duration of Approval

(U) The authority for an NSL remains valid until the information requested is fulfilled.

18.6.6.3.7 (U) Specific Procedures

(U//FOUO) A cover EC that documents the relevance of the information sought and the need for non-disclosure (if a non-disclosure provision is included in the NSL) must accompany all NSLs. All NSLs, with limited exceptions discussed below, must be created on the NSL subsystem to the FISA Management System (FISAMS). The EC must reference an investigative file—not a control file—to which the information sought is relevant.

(U//FOUO) The NSL subsystem allows for the web-based creation of NSLs and supporting ECs. Use of the subsystem ensures that the information in the NSL is consistent with the

EXHIBIT 21

b6 -1
b7C -1

CLASSIFIED BY: NSICG
REASON: 1.4 (C)
DECLASSIFY ON: 12-31-2042
DATE: 07-10-2018

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~

(U) Best Practices for Media Policy

(U) Context

(U//~~FOUO~~) Media Policy (28 CFR 50.10) requires approval from DOJ ("Media Policy Consultation") for the use of interviews/compulsory process on a news media member relating to an offense committed in the course of, or arising out of, newsgathering activities. In the policy, compulsory process is specified as grand jury subpoenas, 2703D or 3123 court orders, and criminal search warrants [redacted] b7E -10

[redacted] b1 -1
b3 -1
b7E -10,11

~~(S//NF~~ [redacted]

[redacted] (S)

(U//~~FOUO~~) Procedures

b1 -1
b3 -1
b7E -10,11

~~(S//NF~~ [redacted]

(S) [redacted]

~~(S//NF~~ [redacted] b1 -1
b3 -1
b7E -3

~~(S//NF~~ [redacted] b1 -1
b3 -1
b7E -10

(S) [redacted]

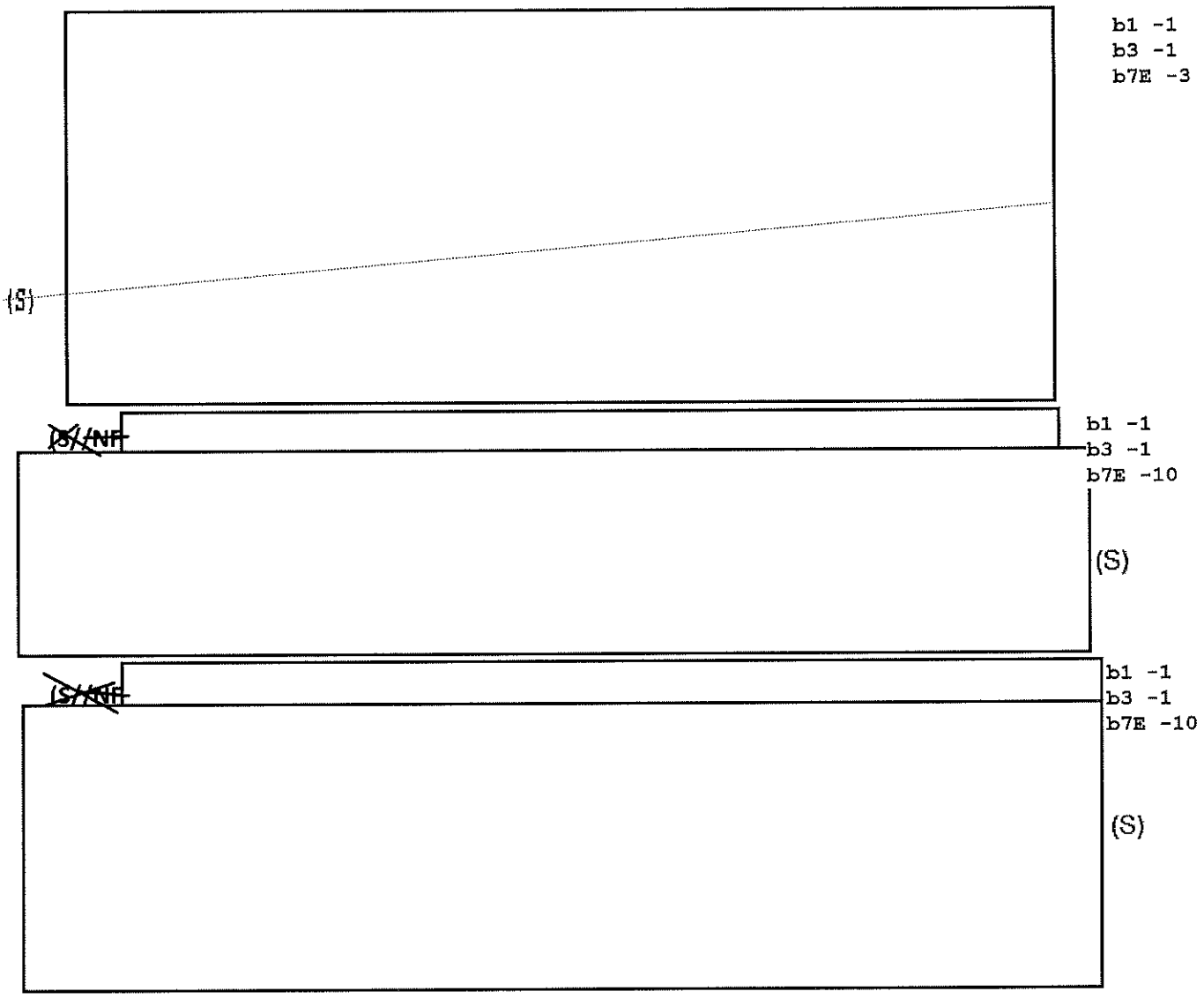
(U//~~FOUO~~) Background should be a concise explanation of the case, including the predication and the 5Ws.

~~(S//NF~~ [redacted] (S) b1 -1
b3 -1
b7E -10

Classified By: [redacted]
Derived From: ~~FBI NSIC dated 20130301~~
Declassify On: ~~20421231~~

b6 -1
b7C -1

~~SECRET//NOFORN~~



(U) Request for Review should request DOJ Policy and Statutory Enforcement Unit (PSEU) to review the LHM and provide a response (see Points of Contact below).

~~SECRET//NOFORN~~

(U//~~FOUO~~) Media Policy Consultation LHMs should be addressed to:

To: [redacted]

b6 -1
b7C -1

Office of Enforcement Operations
Criminal Division
Department of Justice

Attn: [redacted]

b6 -1
b7C -1

Policy and Statutory Enforcement Unit

(U) Points of Contact

DOJ/CRIM/OEO/PSEU (Main Number [redacted]

b6 -1
b7C -1

[redacted] (U)
[redacted] (TS)

[redacted]

b6 -1
b7C -1

[redacted] U)
[redacted] TS)

(U) Tips

(U) Remember the "garbage in, garbage out" principle. If your LHM is incomplete, incoherent, or unpersuasive, it will likely be returned for edits and resubmission.

(U) Approved Examples

(U) [redacted]
(U) [redacted]

b3 -1
b7E -1,2

~~SECRET//NOFORN~~

EXHIBIT 22

DECLASSIFIED BY: NSICG [redacted]
ON 07-10-2018

b6 -1
b7C -1

National Security Letters

[INSERT LOCATION] Field Office
[INSERT DATE]

[redacted]

b6 -1
b7C -1

National Security Law Branch, FBI Headquarters

[redacted]

FBI(17cv9343)-774

Case 1:17-cv-09343-JGK Document 52-22 Filed 02/21/20 Page 3 of 3

UNCLASSIFIED BY: NSICG [redacted]
ON 07-10-2018

Telephone Toll Billing Records of Members of Media & News Organizations

b6 -1
b7C -1

- Investigation of members of media and news organizations is a sensitive investigative matter.

b7E -6,-9

[redacted]

- DIOG – Appendix G: Classified Provisions

EXHIBIT 23

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

MAR 05 2018

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

This responds to your letter to the Attorney General dated October 10, 2017, in which you seek information regarding the Department of Justice's (Department) use of law enforcement tools to gather evidence regarding communications by members of the news media in conducting investigations of leaks. You have also asked about changes to Department policy and procedures regarding obtaining information involving members of the news media.

The Department takes very seriously the important role of the free press in our nation. As you note, in 2015, the Department revised its policy to strike a balance among several vital interests: protecting national security, ensuring public safety, promoting effective law enforcement and the fair administration of justice, and safeguarding the essential role of the free press in fostering government accountability and an open society. The Department's policy is reflected in the Code of Federal Regulations, 28 C.F.R. § 50.10, and the United States Attorneys' Manual (USAM), USAM 9-13.400. As implemented, the policy has achieved a balance through centralized and vigorous internal review of requests for authorization to use law enforcement tools. Although the Department is currently reviewing our policies, there have been no revisions to the existing policy and procedures since January 20, 2017.

Your letter requests the number of instances over the past five years in which the Department has used law enforcement tools to obtain communications records, geolocation information, and the contents of communications. Below we provide responses to your specific requests for information from January 2012 to the present:

- In 2013, in an investigation concerning the unauthorized disclosure of national security information, the Attorney General authorized the issuance of subpoenas and the submission of an application for a court order, pursuant to 18 U.S.C. § 2703(d), for non-content communications records of members of the news media.[1] The subpoenas were issued; the 2703(d) order was vacated.

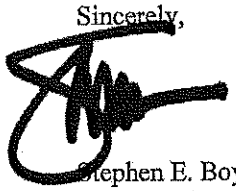
[1] Per the Department's policy, "communications records" include "the contents of electronic communications as well as source and destination information associated with communications, such as email transaction logs and local and long distance telephone connection records, stored

- In 2014, in connection with the prosecution of Jeffrey Sterling for offenses related to his unauthorized disclosure of national security information, the Attorney General authorized federal prosecutors to issue a subpoena to *New York Times* reporter James Risen for limited trial testimony. Risen testified at a pretrial hearing, but was not called to testify at trial. This subpoena is reflected in the 2014 Annual Report Regarding Department of Justice Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media (copy enclosed). *See* USAM 9-13.400(L)(4)(providing that the Department will prepare on an annual basis a public report regarding the use of law enforcement tools covered by the policy).

- The Federal Bureau of Investigation does not currently use national security letters to advance media leak investigations.

We hope that this information is helpful. Please do not hesitate to contact me if we may provide additional assistance regarding this or any other matter.

Sincerely,



Stephen E. Boyd
Assistant Attorney General

Enclosure

---

or transmitted by a third-party communication service provider with which the member of the news media has a contractual relationship." 28 C.F.R. § 50.10(b)(3)(i)(A).

Department of Justice Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media

Annual Report: Calendar Year 2014

By memorandum dated February 21, 2014, the Attorney General committed to making public, on an annual basis, data regarding the Department's use of certain law enforcement tools to obtain information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media, pursuant to 28 C.F.R. § 50.10. This public report, which encompasses authorizations during calendar year 2014, is derived from information provided by Department Divisions and United States Attorneys' Offices (USAOs).

A. Subpoenas and applications for court orders or search warrants authorized by the Attorney General (28 C.F.R. §§ 50.10(c) and (d)):

1. In connection with the trial of former CIA officer Jeffrey Sterling, who was charged with, and convicted of, offenses related to his unauthorized disclosure of national security information, the Attorney General authorized the Criminal Division and the USAO for the Eastern District of Virginia to issue a subpoena to *New York Times* reporter James Risen. The authorization was limited to eliciting testimony at trial and/or pretrial hearings confirming (1) that Risen has a confidentiality agreement with a particular source, (2) that Risen authored a particular chapter in his book *State of War*, (3) that statements attributed to an unnamed source were, in fact, made by an unnamed source, (4) that statements attributed to an identified source were, in fact, made by an identified source, and (5) the existence of a prior non-confidential reporter-source relationship with Sterling.

   Pursuant to the Department's policy, the Director of National Intelligence certified to the Attorney General "the significance of the harm raised by the unauthorized disclosure and that the information disclosed was properly classified" and reaffirm[ed] "the intelligence community's continued support for the . . . prosecution." 28 C.F.R. § 50.10(c)(4)(vi). In addition, the Attorney General considered the recommendations of both the Criminal Division and the News Media Review Committee.

   The subpoena was issued, and Risen testified at a pretrial hearing. He was not called to testify at trial.

2. The Attorney General authorized the USAO for the Southern District of New York to issue a subpoena to a television news producer for testimony and the production of documents in connection with the trial of Khalid al Fawwaz, who was charged with, and convicted of, various offenses related to the August 7, 1998 bombings of the United States embassies in Kenya and Tanzania. The contemplated testimony related to allegedly anti-American and anti-Semitic

statements al Fawwaz made to the prospective witness while al Fawwaz was serving as Usama bin Laden's representative to the media around the time of the bombings of the embassies. After the prospective witness made clear that he would contest a subpoena, members of the Department engaged in further negotiations with counsel for the prospective witness and decided to hold the issuance of the subpoena in abeyance pending assessment of the evidence introduced at trial. Ultimately, the USAO did not issue the subpoena.

3. In an investigation regarding the theft of proprietary information, the Attorney General authorized a USAO to submit an application for a warrant to search the home and electronic media of an individual suspected of making an unauthorized intrusion into a protected database (i.e., hacking), but whom the Department treated as a member of the news media in an abundance of caution. The Attorney General took into consideration the recommendations of both the Criminal Division and the News Media Review Committee. Consistent with the Department's policy, the authorization directed the use of certain search and safeguarding protocols. Ultimately, federal investigators opted not to execute the warrant.

B. Questioning, arrests, or charges authorized by the Attorney General (28 C.F.R. § 50.10(f)):

1. In connection with a national security investigation, the Attorney General authorized federal investigators to question a member of the news media. Pursuant to the Department's policy, such questioning was voluntary, and was not compelled pursuant to a subpoena or other process.

2. In connection with an investigation, the Attorney General authorized federal agents to question an individual whom the Department treated as a member of the news media. Pursuant to the Department's policy, such questioning was voluntary, and was not compelled pursuant to a subpoena or other process.

C. Subpoenas, applications for court orders or search warrants, questioning, arrests, or charges authorized by a Deputy Assistant Attorney General for the Criminal Division (28 C.F.R. §§ 50.10(d)(4) and (g)):

None.

D. Subpoenas and applications for court orders authorized by Assistant Attorneys General or United States Attorneys (28 C.F.R. § 50.10(c)(3)):

1. In a civil investigation, the Assistant Attorney General for the Antitrust Division authorized the issuance of civil investigative demands (CIDs) to two news media entities for copies of the entities' organization charts, personnel directories, and related information; and information relating to the restructuring of the entities' joint ownership of a publishing entity. The information sought constitutes "purely

commercial, financial, administrative, technical, or other information unrelated to newsgathering activities" or "information or records relating to personnel not involved in newsgathering activities." 28 C.F.R. § 50.10(c)(3)(ii)(A). The news media entities complied with the CIDs.

2. In a tax-related prosecution of an employee of a news media entity, a United States Attorney authorized the issuance of a subpoena to a news media entity for the defendant-employee's employment records, tax records, and financial transaction records. The information sought constitutes "purely commercial, financial, administrative, technical, or other information unrelated to newsgathering activities" or "information or records relating to personnel not involved in newsgathering activities." 28 C.F.R. § 50.10(c)(3)(ii)(A). The news media entity complied with the subpoena.

3. A United States Attorney authorized the issuance of a subpoena to a news media entity for audio and video recordings related to a broadcast report that contained information relevant to a criminal investigation of an individual who is not a member of the news media. The news media entity expressly agreed to provide the requested recordings in response to a subpoena. *See* 28 C.F.R. § 50.10(c)(3)(i)(A).

4. In connection with the prosecution of Dzhokhar Tsarnaev for offenses related to his role in the 2013 Boston Marathon bombings and the aftermath, the United States Attorney for the District of Massachusetts authorized the issuance of trial subpoenas to CNN and WBZ-TV for audio and video recordings of the finish line. CNN and WBZ-TV expressly agreed to provide the requested recordings in response to subpoenas. *See* 28 C.F.R. § 50.10(c)(3)(i)(A).

5. A United States Attorney authorized the issuance of a subpoena to a news media entity for a video recording of an interview of a target of a criminal investigation. The entity expressly agreed to provide the requested recording in response to a subpoena. *See* 28 C.F.R. § 50.10(c)(3)(i)(A).

6. In connection with the prosecution of Roger Key for conspiracy to commit murder-for-hire, attempted murder-for-hire, and aiding and abetting the unlawful discharge of a firearm, the United States Attorney for the Southern District of New York authorized the issuance of a subpoena to a news media entity for the broadcast footage of, and script for, a report concerning a related murder. The news media entity expressly agreed to provide the requested recordings in response to a subpoena. *See* 28 C.F.R. § 50.10(c)(3)(i)(A). Ultimately, the news media entity failed to respond to the subpoena. However, while the subpoena was pending, the USAO negotiated with the defense a stipulation regarding the admissibility of the publicly broadcast report.

7. In connection with the prosecution of William White for making threats to a reporter, the United States Attorney for the Middle District of Florida authorized

the issuance of a subpoena to the victim's employer for trial testimony authenticating materials (i.e., copies of the threats -- some of which were posted on the news media entity's website) that the news media entity previously had provided to state law enforcement authorities voluntarily (i.e., without a subpoena), who then provided the materials to federal authorities. The information sought "related to public comments, messages, or postings by readers, viewers, customers, or subscribers, over which the member of the news media did not exercise editorial control prior to publication," and the news media entity expressly agreed to provide the requested information in response to a subpoena. 28 C.F.R. §§ 50.10(c)(3)(i)(A) and (B).

EXHIBIT 24

18.6.6.3.2 (U) Definition of Method

(U) An NSL is an administrative demand for documents or records that are relevant to a Predicated Investigation to protect against international terrorism or clandestine intelligence activities. [redacted] b7E -1

18.6.6.3.3 (U) Approval Requirements

(U//~~FOUO~~) Those who approve NSLs are responsible for ensuring the investigative and procedural requirements have been met. They must certify that the information sought by the NSL is relevant to an open, predicated national security investigation. For an NSL to include a nondisclosure provision, the approver must determine that disclosure of the NSL may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person. Those who approve NSLs, as well as those designated as acting officials who will approve NSLs, must have completed the Virtual Academy course on NSLs, reviewed DIOG Section 18.6.6. (National Security Letter), and if appropriate, received NSL training from the CDC/ADC or a National Security Law Branch (NSLB) attorney prior to approving NSLs.

(U//~~FOUO~~) The process for creating an NSL involves two documents: the NSL itself and the EC approving the issuance of the NSL. The Director has delegated the authority to sign NSLs to the Deputy Director, Executive Assistant Director, and Associate EAD for the National Security Branch; Assistant Directors and all DADs for the Counterterrorism, Counterintelligence, and Cyber Divisions, and the Weapons of Mass Destruction Directorate; General Counsel; Deputy General Counsel for the National Security Law Branch; Assistant Directors in Charge in New York, Washington, DC, and Los Angeles; and all SACs in all field offices. See EC 333-HQ-A1487720 Serial 515 (May 15, 2012). No other *delegations* are permitted. However, the authority to approve NSLs may be designated to an acting official (see below).

(U//~~FOUO~~) [redacted] b7E -1

[redacted]

(U//~~FOUO~~) In addition to being signed by a statutorily required approver, an NSL must be approved by a CDC, ADC (or attorney acting in that capacity), or an NSLB attorney.

18.6.6.3.4 (U) Standards for Issuing NSLs

(U//~~FOUO~~) [redacted] b7E -1

[redacted]

epic.org EPIC-17-06-13-FBI-FOIA-20190225-Production-pt1 000005
FPF-89