



**U.S. Department of Justice**

*United States Attorney  
Southern District of New York*

---

*86 Chambers Street  
New York, New York 10007*

May 29, 2015

By Electronic Mail

David E. McCraw, Esq.  
Jeremy A. Kutner, Esq.  
The New York Times Company  
620 Eighth Avenue  
New York, NY 10018  
E-mail: mccrad@nytimes.com  
jeremy.kutner@nytimes.com

Re: *The New York Times Co. v. U.S. Department of Justice*, 14 Civ. 3948 (VSB)

Dear David and Jeremy:

This Office represents the United States Department of Justice ("DOJ"), the defendant in the above-referenced matter. DOJ has completed its review and processing of documents in accordance with the schedule set forth in the Stipulation and Order Regarding Additional Processing and Briefing, dated March 30, 2015 (the "Stipulation").

With respect to paragraph 1 of the Stipulation, DOJ identified three memoranda of law, and is releasing them with redactions as three separate .pdf documents. With respect to paragraph 2 of the Stipulation, DOJ identified one memorandum of law and one order, and is releasing them with redactions, combined into one .pdf document. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), (b)(6), (b)(7)(A), and (b)(7)(E). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

With respect to paragraph 3, DOJ can neither confirm nor deny the existence of any documents responsive to categories 12 or 13 of the FOIA Request, as defined in the Stipulation.

These documents will be made available to the public on Monday, June 1, 2015, on the Director of National Intelligence's website, "IC on the Record," at <http://icontherecord.tumblr.com/>, as well as at [www.dni.gov](http://www.dni.gov).

If you have any questions, please do not hesitate to contact us.

Sincerely,

PREET BHARARA  
United States Attorney for the  
Southern District of New York

By: /s/ Emily E. Daughtry  
JOHN D. CLOPPER  
EMILY E. DAUGHTRY  
ANDREW E. KRAUSE  
Assistant United States Attorneys  
Telephone: (212) 637-2716/2777/2769  
Facsimile: (212) 637-0033  
E-mail: john.clopper@usdoj.gov  
emily.daughtry@usdoj.gov  
andrew.krause@usdoj.gov

Enclosures



U.S. Department of Justice

National Security Division

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

2007 APR 20 PM 12:41

Office of the Assistant Attorney General

Washington, D.C. 20530

KAREN SUTTON  
CLERK

April 20, 2007

## MEMORANDUM

TO: Honorable Roger Vinson, Judge  
U.S. Foreign Intelligence Surveillance Court

FROM: Kenneth L. Wainstein *Ken Wainstein / Melsen*

SUBJECT: Report in No. [REDACTED]

On March 21, 2007, the Government filed an application, Docket No. [REDACTED] under the electronic surveillance provisions of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1811, seeking renewal of the surveillance authority for the National Security Agency granted in Docket No. [REDACTED]. Like the application in No. [REDACTED] this application identified the "target" of the proposed surveillance as [REDACTED] foreign powers: [REDACTED]

[REDACTED] The application identified the "facilities" at which the surveillance was to be directed [REDACTED]

[REDACTED] It also proposed minimization procedures that would have required the Government to report to the Court every 30 days concerning new telephone numbers and e-mail addresses used by NSA as foreign selectors. It did not require the Court make probable cause determinations with respect to individual existing or new foreign selectors. ~~(TS//SI//NF)~~

On March 29, you advised us that you had reservations about the legal theory advanced in the Government's application. You then issued an Order and Memorandum Opinion setting forth your reasoning on April 3. In your Opinion, you did not take issue with our identification of the targets of the proposed electronic surveillance as the [REDACTED] foreign powers noted above. But you concluded that the facilities at which the surveillance is directed are the individual telephone numbers and e-mail addresses used by NSA as selectors and found the application inadequate under FISA because it did not provide a probable cause justification for each selector. In addition, you expressed concern that our proposed reporting procedure was contrary to the language of FISA in that it provided for after-the-fact reporting rather than prior judicial authorization. Thus, you found that our proposed minimization procedures did not meet the definition of such procedures under section 1801(h):

Understanding our need for time to address your concerns, you allowed us to seek—and we obtained—an extension of the authorization granted in No. [REDACTED] until 5 p.m. on May 31, 2007. You instructed us to "periodically submit written reports . . . regarding [our] efforts to prepare and submit for [your] consideration a revised and supplemented application that would

~~TOP SECRET//SI//NF~~

meet the requirements of FISA as described in [your] order and opinion." This memorandum constitutes the first such report, which is due on or before April 20, and sets forth a new proposal that we have crafted to address the concerns you expressed in your Opinion and in our meetings.

~~(TS//SI//NF)~~

*New Approach: After-acquired/Roving Surveillance (U)*

Since receiving your Opinion, we have examined FISA closely to determine whether there are alternate approaches, anchored in the clear terms of FISA as interpreted in your Opinion, that would allow the Government the speed and agility needed to serve the same early warning function as the surveillance authorized in No. [REDACTED]. We believe that we have developed such an approach, which is significantly different from the approach contained in our prior submission.

Our proposal has two parts. First, unlike our prior submission, this new approach would require the Court, in considering the application, to make a probable cause finding that each of the [REDACTED] telephone numbers and e-mail addresses included in the application and currently targeted for collection under No. [REDACTED] is being used or is about to be used by [REDACTED] targets of the surveillance. Second, for numbers and addresses NSA discovers after the Court grants the application, the new approach relies on those provisions of FISA, and Court practice under them, which allow the Court to authorize the Government to initiate surveillance of new facilities (e.g., telephone numbers and e-mail addresses) used by the same target that the Government identifies after the initial authorization. This authority accounts for targets like the foreign powers here that [REDACTED]. When the Government uses this authority, it must comply with a statutory reporting requirement. That provision, which applies when the nature and location of the facilities at which the surveillance is directed is "unknown" at the time of the application, requires the Government to report the new facility and the probable cause supporting the surveillance of it to the Court within ten days. Also unlike the prior approach, this approach will require the Court to make probable cause determinations with respect to each of the new telephone numbers and e-mail addresses at, or before, renewal. Should the Court agree that this approach is consistent with the statute, we will continue to work with NSA to ensure that it can be accomplished in light of the Government's logistical constraints and in a manner consistent with the operational purpose of the surveillance.

~~(TS//SI//NF)~~

Like the application in No. [REDACTED] this application would seek authority to conduct surveillance of these foreign powers by tasking for collection only telephone numbers and e-mail addresses reasonably believed to be used outside the United States. It recognizes that these powers operate in a multitude of foreign countries, [REDACTED] to avoid detection. ~~(TS//SI//NF)~~

*Proposed Application for After-acquired/Roving Authority (U)*

Our proposed application would be structured as follows:

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

- We would continue to identify the targets of the electronic surveillance as the [REDACTED] foreign powers noted above. (TS//SI//NF)
- We would identify, as your Opinion does, the “facilities . . . at which the electronic surveillance is directed,” § 1804(a)(4)(B), as the individual telephone numbers and e-mail addresses that NSA tasks for collection. (TS//SI//NF)
- For each of the foreign selectors currently under surveillance, we would submit for the Court’s review “a statement of the facts and circumstances relied upon by the [Government] to justify [its] belief that . . . each of the facilities . . . at which the electronic surveillance is directed is being used, or is about to be used, by” [REDACTED] identified foreign powers. *Id.* You would then review these facts and circumstances for each of the telephone numbers and e-mail addresses to determine whether probable cause exists. *See id.* § 1805(a)(3)(B). (TS//SI//NF)
- We have sent attorneys from the National Security Division (NSD) to NSA to help prepare revised and updated probable cause submissions for these [REDACTED] facilities. NSD attorneys are working side-by-side with NSA professionals. Together, they are working to modify NSA’s existing documentation of each justification—which in most cases was initially prepared for NSA’s internal use only—for each facility. With guidance from NSD attorneys, NSA is in the process of reviewing each probable cause submission so that the necessary facts can be provided to the Court in one clear and concise statement. A sample of our probable cause submissions is attached as Exhibit A. (TS//SI//NF)
- As we did in our prior application, we would submit the facts and circumstances that underlie our conclusion that [REDACTED] have other telephone numbers and e-mail addresses that are unknown to NSA at the time of the application, that they will acquire new telephone numbers and e-mail addresses during the period of surveillance, [REDACTED] (TS//SI//NF)

*Proposed Order Authorizing Surveillance (U)*

If you were satisfied that probable cause existed to conduct electronic surveillance of all or a portion of the specified known facilities and that the statutory requirements were otherwise met, you would issue an order authorizing the surveillance, as follows. *See id.* § 1805. (U)

- The Order would specify “the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.” *Id.* § 1805(c)(1)(B). That is, the Order would specify the telephone numbers and e-mail addresses for which the Court had found probable cause. (TS//SI//NF)
- The Order would also recognize that there are facilities used by the targeted foreign powers whose “nature and location” is not “known.” *See id.* FISA provides for just such

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

a circumstance. "[W]here the nature and location of each of the facilities or places at which the surveillance will be directed is unknown," FISA requires the Order to direct the Government to "provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility . . ." *Id.* § 1805(c)(3). Such notice must include "the nature and location of each new facility or place at which the electronic surveillance is directed" and "the facts and circumstances relied upon by the [Government] to justify [its] belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance." *Id.* The Order would direct us to provide the Court with such notice. (TS//SI//NF)

- At renewal, the Court would review the facts and circumstances provided in the notice as to each surveillance and determine whether probable cause exists for each new facility and the new surveillance may continue. The Court could call for earlier review as well. Section 1805(c)(3)(C) provides that the Government may propose new minimization procedures in its notice to account for the new surveillance. The Court could require that such proposed procedures provide for a Court determination of whether probable cause exists for each new facility and thus whether surveillance may continue, without awaiting the renewal application.<sup>1</sup> (TS//SI//NF)

*Consistency with Prior Practice and the Language of the Statute (U)*

This approach builds upon prior FISA practice and is contemplated by the plain language of the statute, both of which evince the Court's power, in the proper case, to authorize the Government to initiate surveillance immediately upon the Government's finding of probable cause in circumstances where it is anticipated that the target will use facilities that are unknown at the time an order is granted authorizing surveillance. As in the case of roving wiretaps in the criminal context, this authorization is critical to the Government's ability to follow the target in real time and to avoid the loss of valuable information. In order to allow for Court oversight of this authority, the statute and the Court require regular reporting after new surveillance has begun. (S)

The Court has a long-standing practice of authorizing the Government, without first returning to the Court for prior approval, to conduct surveillance of telephone numbers, e-mail addresses, and vehicles that the Government later learns are being used by the target of the surveillance.

(b)(1); (b)(3); (b)(7)(A)



<sup>1</sup> Alternatively, the Court could authorize the initial surveillance for a period of less than 90 days and review the probable cause underlying the surveillance of the new facilities at that earlier time.

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

(b)(1); (b)(3); (b)(7)(A)

As noted above, section 1805(c)(1)(B) provides that an Order need not specify the nature or location of facilities that are not "known." *Id.* It thus recognizes the Court's power to authorize surveillance directed at facilities for which the Government learns of probable cause after the initial order. In such circumstances, FISA establishes a reporting mechanism to ensure that the Court can conduct informed oversight of the Government's use of this authority. *See id.* § 1805(c)(3). Although the legislative history of the reporting provision indicates that it was enacted to provide a mechanism for Court oversight of the authority granted by the USA PATRIOT Act in section 1805(c)(2)(B), where the "person" who must provide assistance to the Government is unknown at the time of the order, nothing in the language of the statute restricts it to that context only. Rather, it applies whenever "the nature and location of each of the facilities or places at which the surveillance will be directed is unknown." *Id.* § 1805(c)(3). That is the case here. In order to conduct the surveillance of the specified foreign powers effectively, the Government must be able to add new telephone numbers and e-mail addresses, which are unknown at this time, as they are discovered.<sup>2</sup> (~~TS//SI//NF~~)

<sup>2</sup> In developing this new approach, we have discovered that prior applications have not read section 1805(c)(3) to require reporting in the traditional after-acquired context, that is, when the Government can identify in the application all of the "specified persons" to whom the secondary orders would be issued. In addition, these applications have read section 1805(c)(3) to apply only when the Government knows neither the "nature" nor the "location" of the new facility or premises. We believe that this reading of the "nature and location" phrase as including two disjunctive requirements both of which must be met is erroneous. The provision uses "is"—the singular form of the verb "to be"—with respect to the term "nature and location." *Id.* § 1805(c)(3). Thus, the term is a unitary concept that refers to whatever identifiers are necessary to specify the facility or place at which the surveillance will be directed. These identifiers will vary according to the type of the facility or place. Because this reporting provision applies whenever the Government does not know the nature and/or location of each of the facilities or places at which the surveillance will be directed, going forward, the Government will follow the

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

Moreover, this approach is consistent with the language of section 1805(c)(2)(B) and the practice thereunder. This section was amended by the USA PATRIOT Act to allow the Court "in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person" whose assistance is required to effect the surveillance to direct that person to provide such assistance. *See id.*<sup>3</sup> When this provision applies, the identity of the directed person is not contained in the application or Order because it is not known at the time. The Government is then provided with the authority to identify that person and require his assistance without first returning to the Court. Under this provision, the Court has authorized the Government [REDACTED]

[REDACTED] within the meaning of section 1805(c)(2)(B). If the target was not the subscriber to the number serviced by the unspecified provider, the FBI in exigent circumstances was authorized to serve a secondary order on the provider for up to 72 hours, after which time the surveillance would have had to have ended unless an OIPR attorney had attested in writing that there was probable cause to believe that the target was using or about to use the [REDACTED]. If the FBI obtained the attestation, the surveillance could continue, subject to a 10-day report to the Court. (TS//SI//NF)

We recognize that the authority we seek to conduct this after-acquired/roving surveillance, although founded in both the plain language of FISA and the Court's prior practice, would allow such surveillance on a greater scale than in the past. In addition, the Government would be given broader discretion than in most prior cases to initiate surveillance of a new facility related to the target, that is, the authorization would not be tied to, e.g. [REDACTED]

[REDACTED] Our proposal, however, does contain significant safeguards and the discretion required stems from the very reason for this program. The surveillance would be only of the targets' telephone numbers and e-mail addresses reasonably believed to be used outside the United States; the Court would have reviewed the probable cause underlying the surveillance of all initial facilities (which would encompass the large majority of the facilities targeted for collection); the Government would be required to report its probable cause findings for new surveillance to the Court within a short period of time; and the Court would review these findings either at, or before, the time of the subsequent renewal application. In light of the size of this program, the scale of the surveillance authorized under any new approach will be unprecedented. And the Government's discretion to begin surveillance on any new facilities is necessary to any program that will provide the Government the needed flexibility to move rapidly to detect the targets' terrorist plots and to foil their attempts at secrecy and evasion.

---

reporting requirement in all applications that seek authorization to initiate surveillance of facilities or premises discovered after the Court's authorization, regardless of whether this surveillance requires the assistance of a "person" different from the one(s) specified in the order.

<sup>3</sup> This provision does not apply directly in this context. Although the targets here [REDACTED] the Government will not [REDACTED]

The Government can [REDACTED]

(TS//SI//NF)

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

Under our approach, any new surveillance would come under the Court's oversight in a matter of days and it would remain supervised thereafter. ~~(TS//SI//NF)~~

\* \* \*

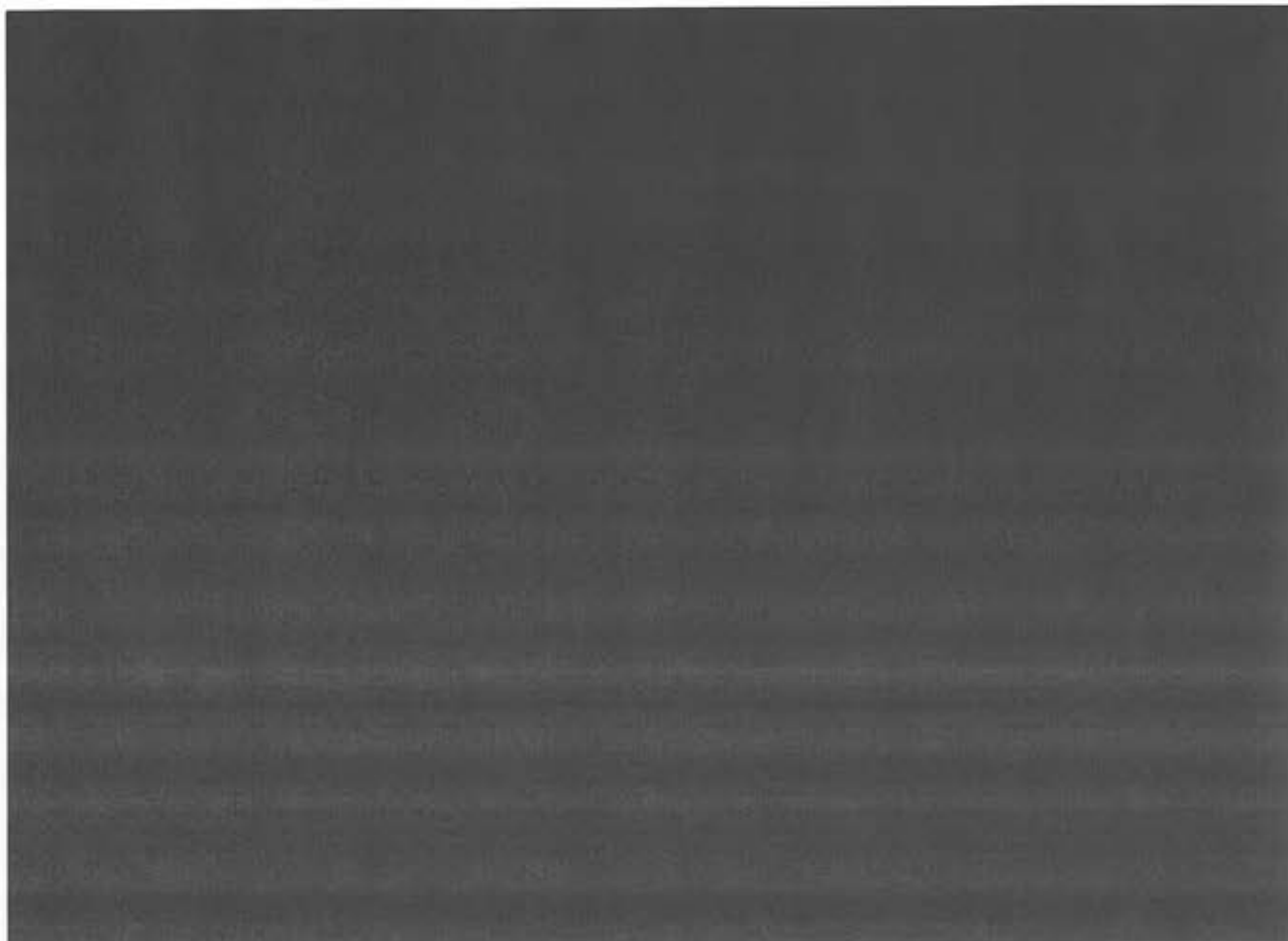
We would like to discuss with you the approach set forth above. We believe that it addresses the concerns you expressed to us, is consistent with FISA and the Court's prior practice, allows the Government the speed and agility it needs to operate this early warning system, and provides for the judicial oversight FISA envisions. We remain committed to developing an approach that satisfies these conditions. Because of the time constraints on pursuing this or other options, we respectfully request that the Court provide us its views on this approach as quickly as possible. ~~(TS//SI//NF)~~

~~TOP SECRET//SI//NF~~

TAB

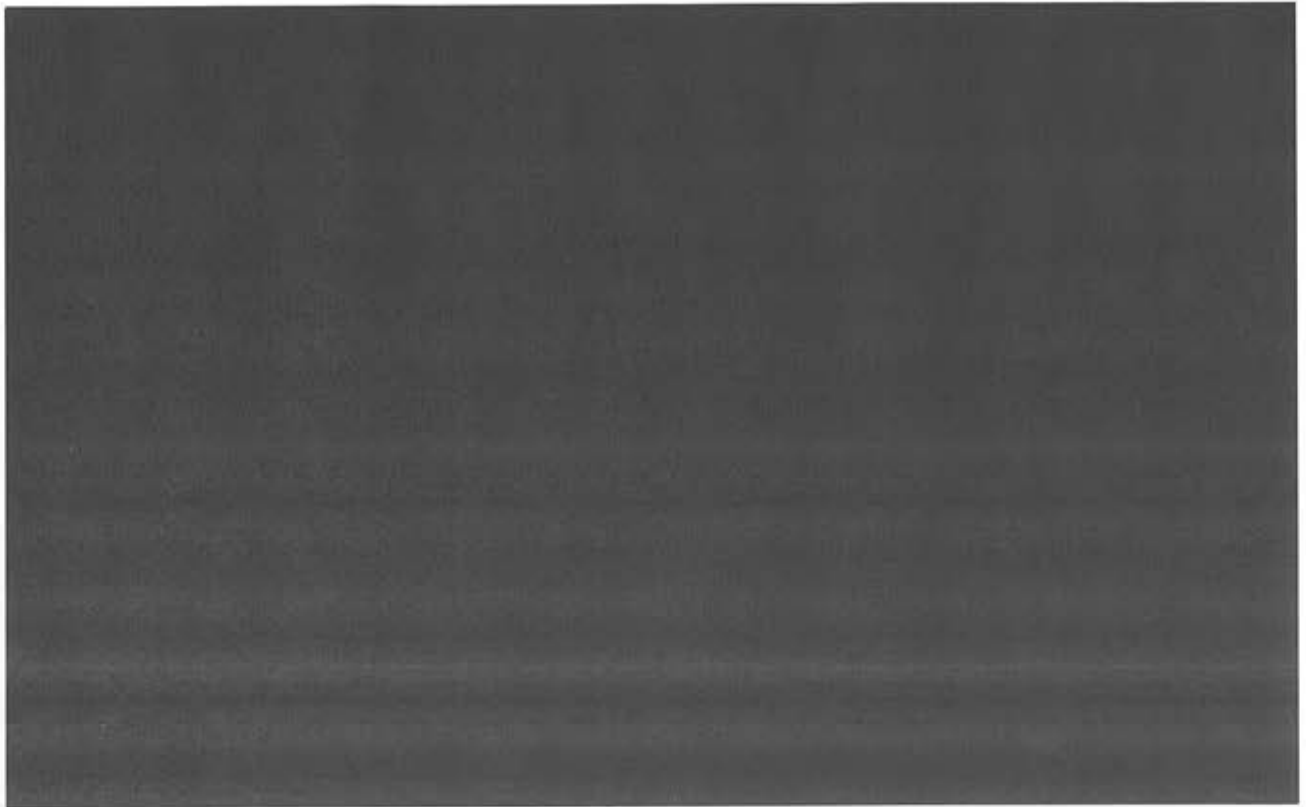
A

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

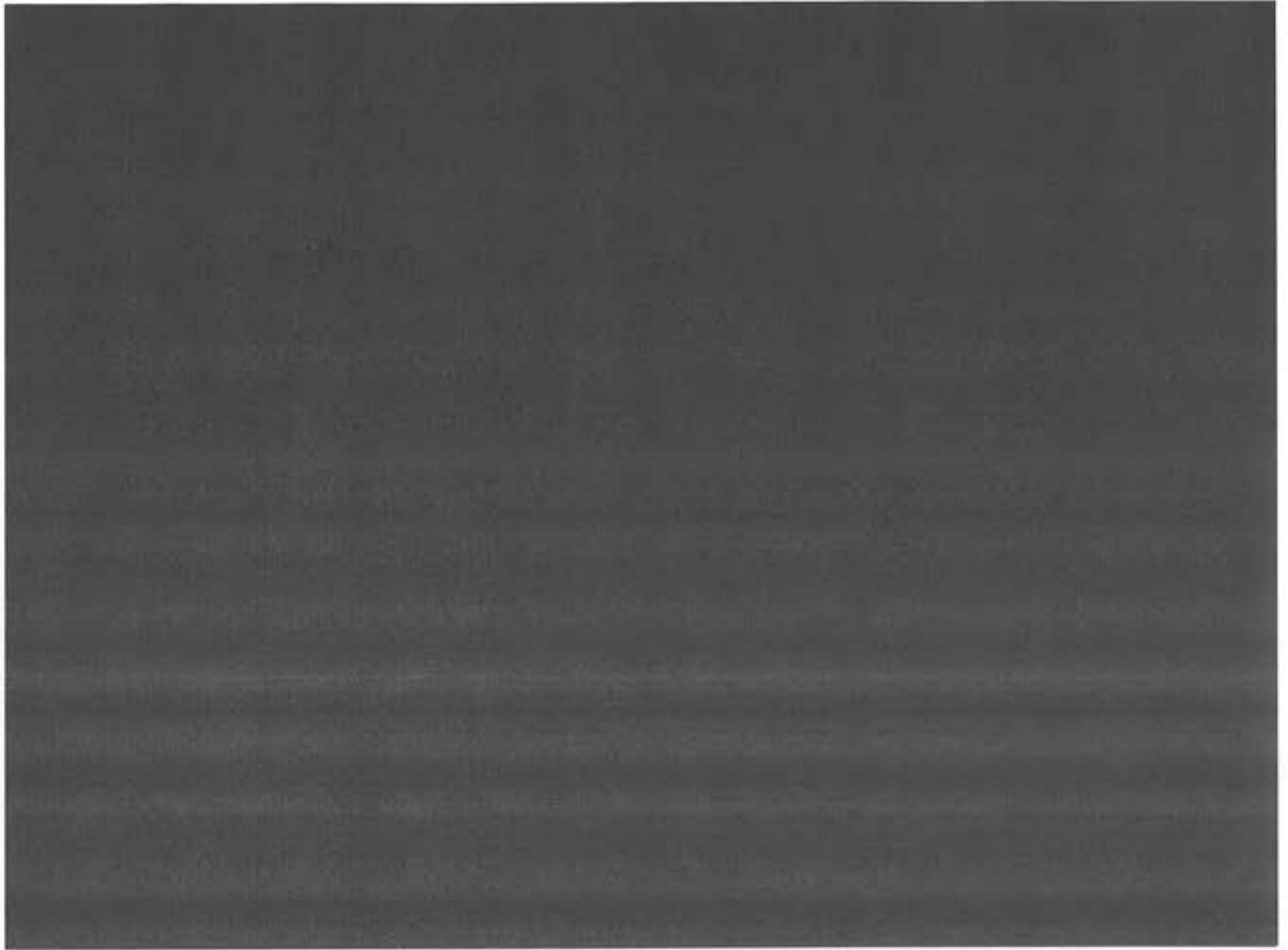
~~TOP SECRET//COMINT//NOFORN//20291123~~

(b)(1); (b)(3); (b)(7)(A)



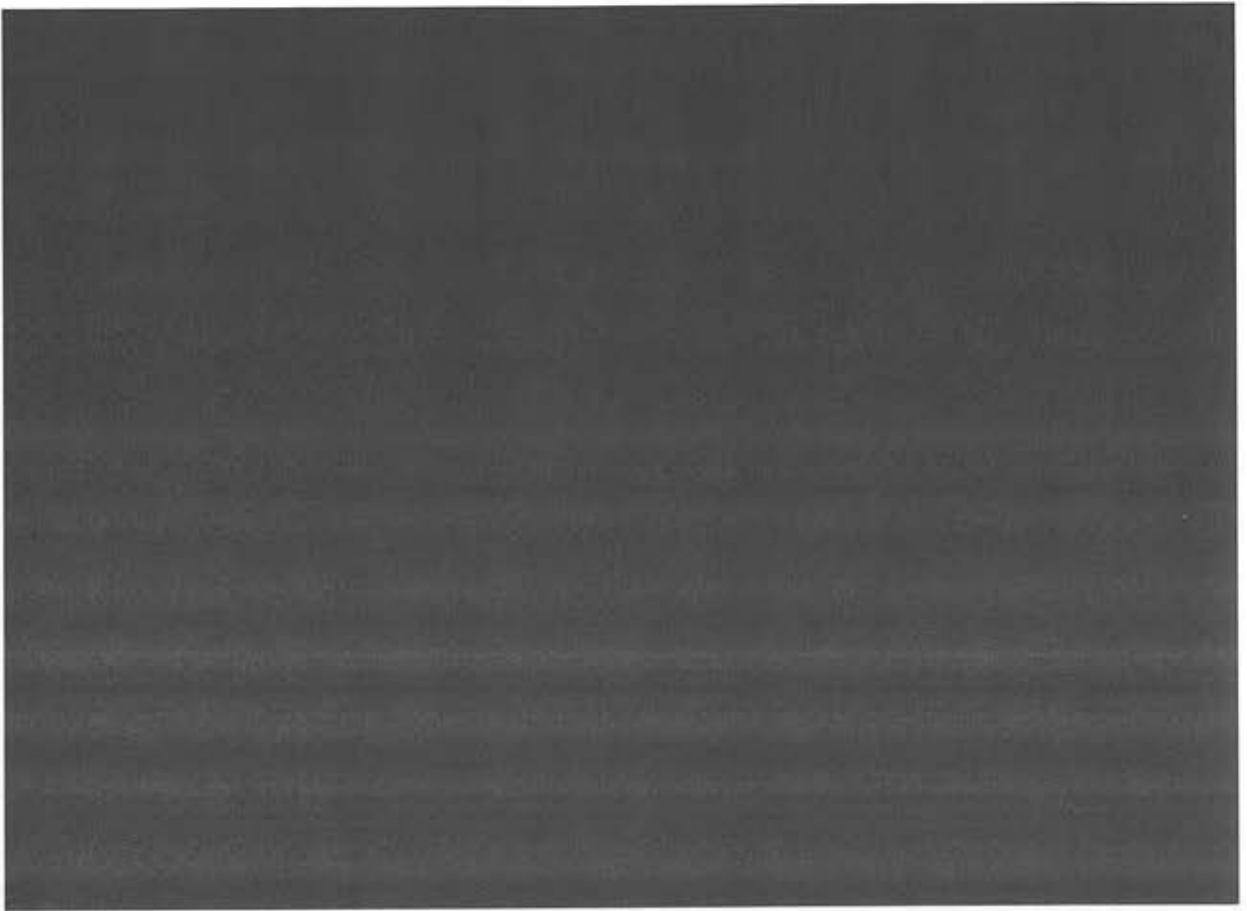
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

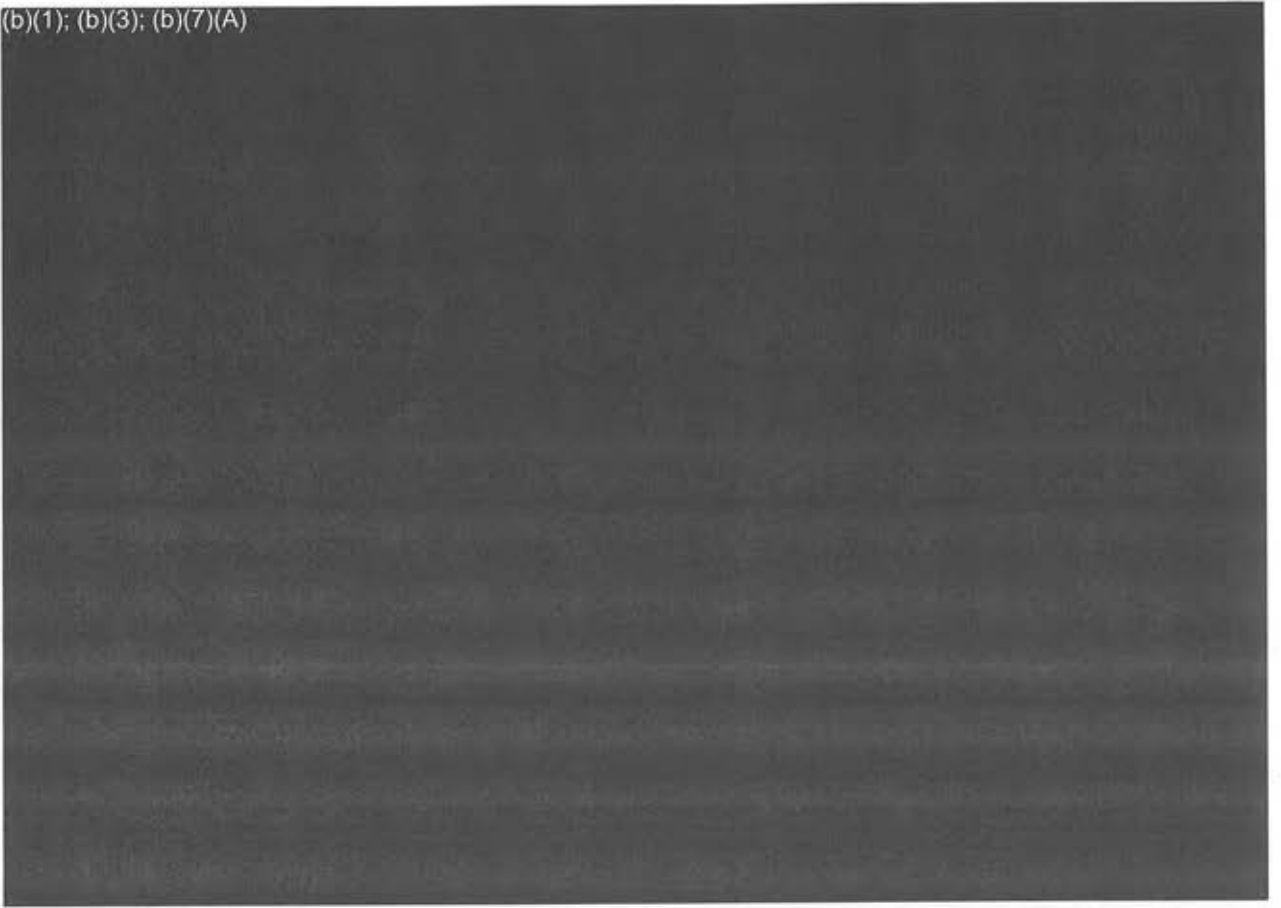
~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

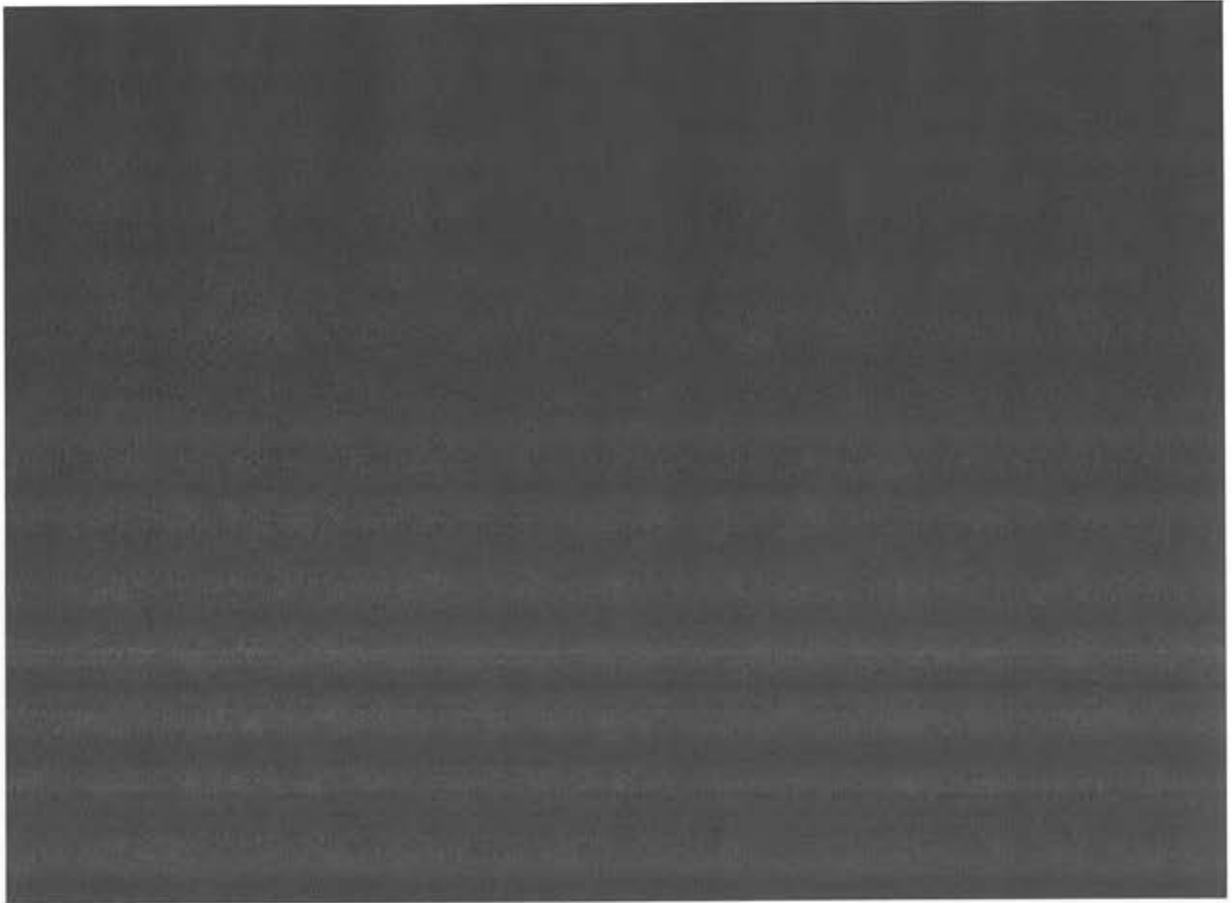
~~TOP SECRET//COMINT//NOFORN//20291123~~

(b)(1); (b)(3); (b)(7)(A)



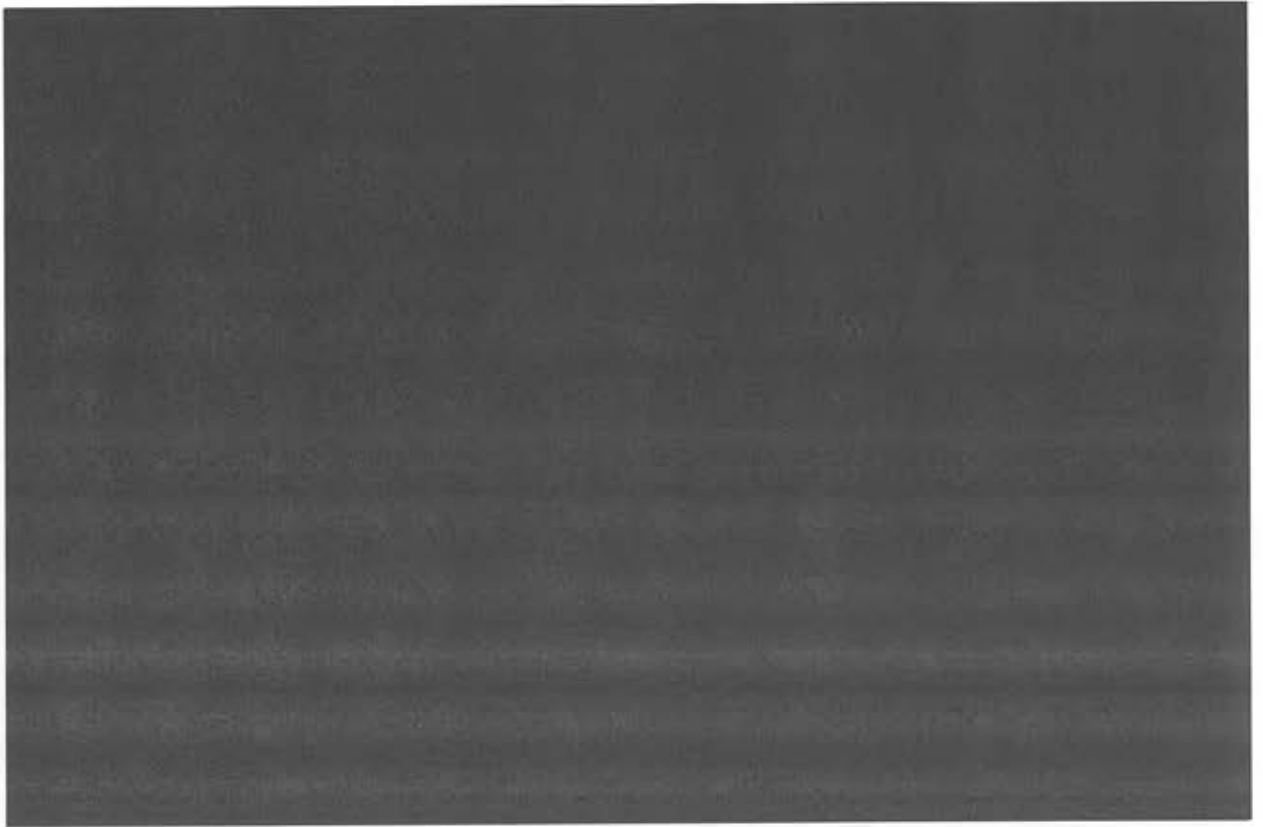
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



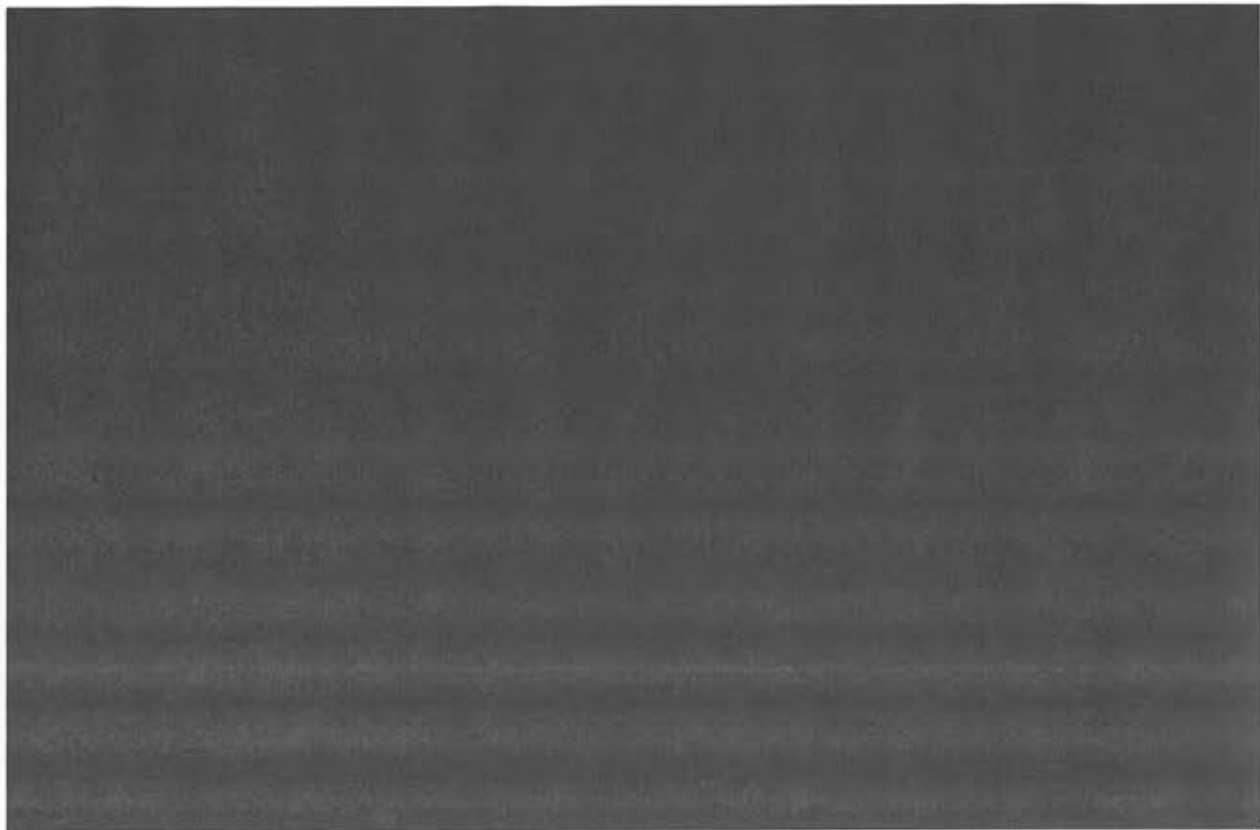
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



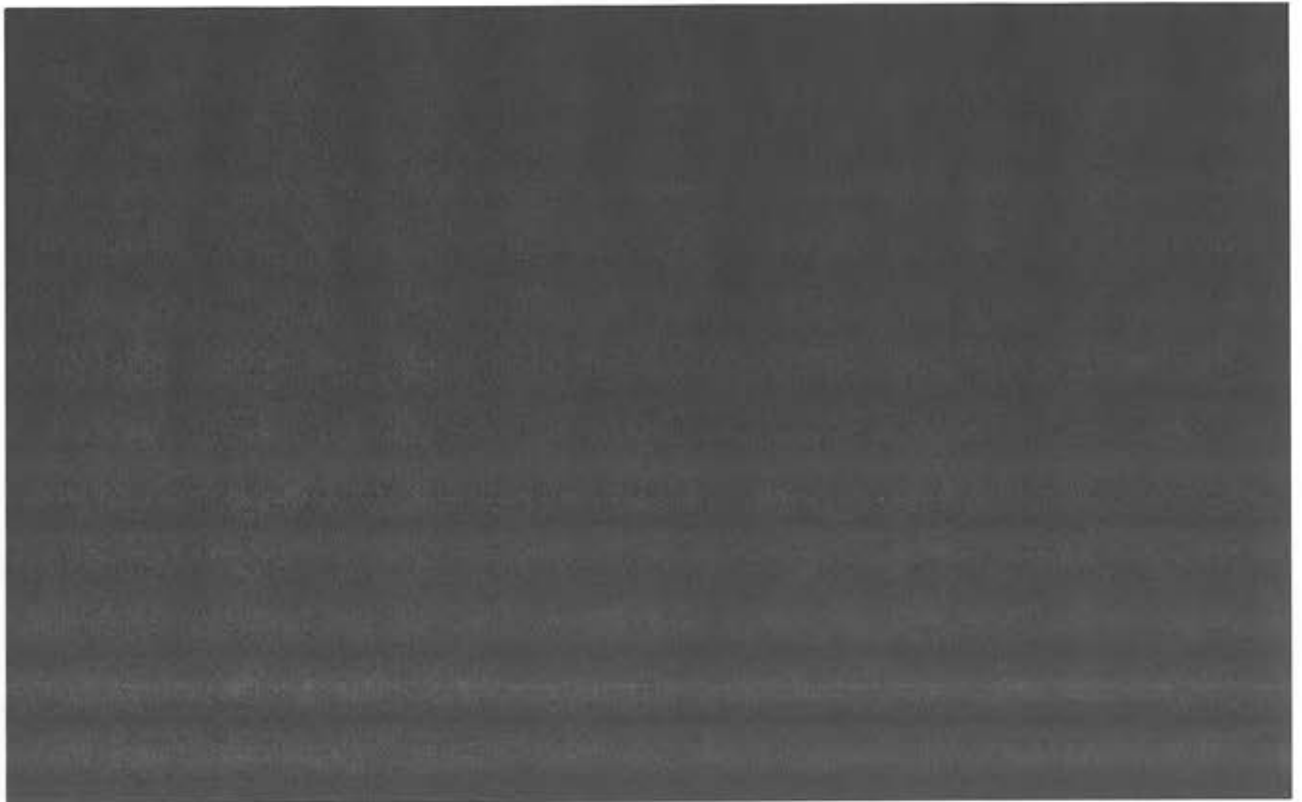
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



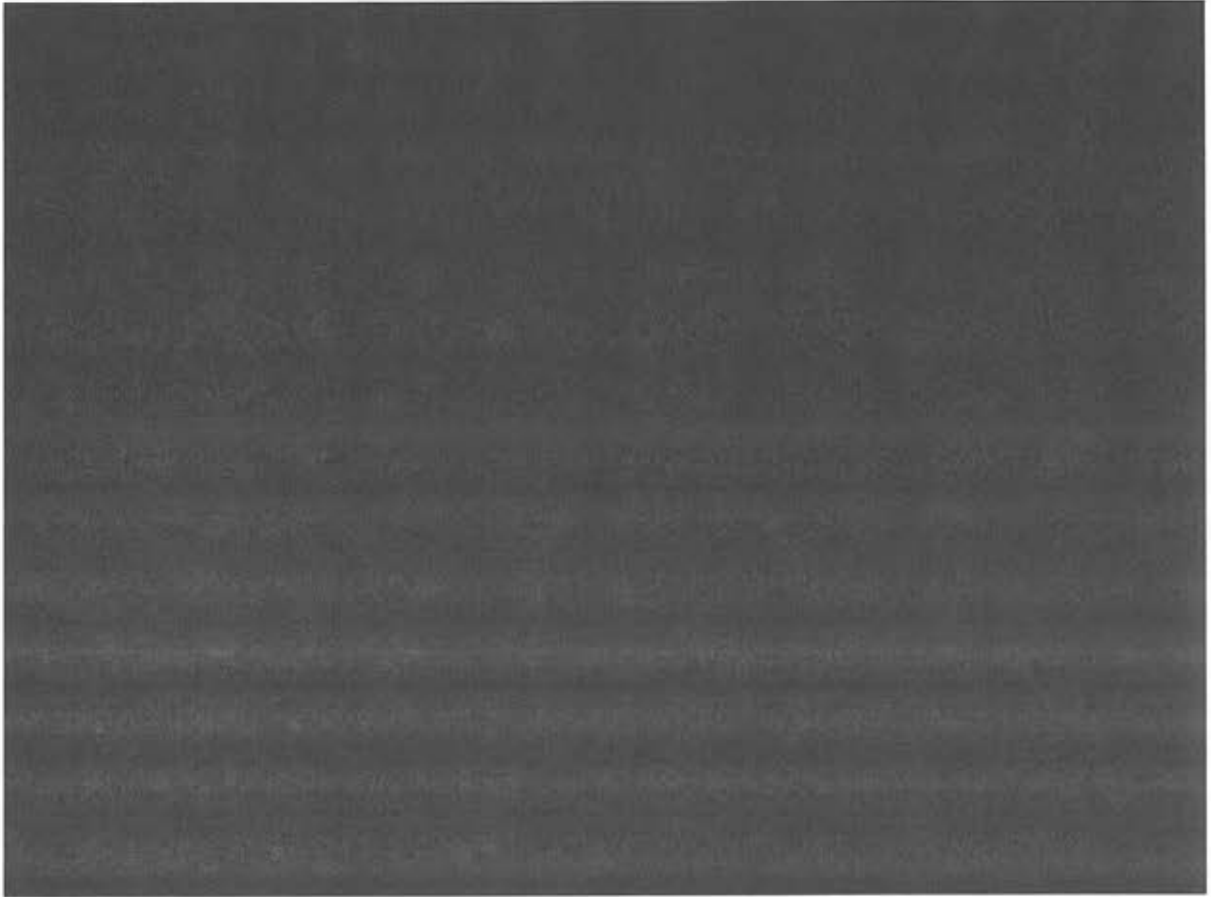
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



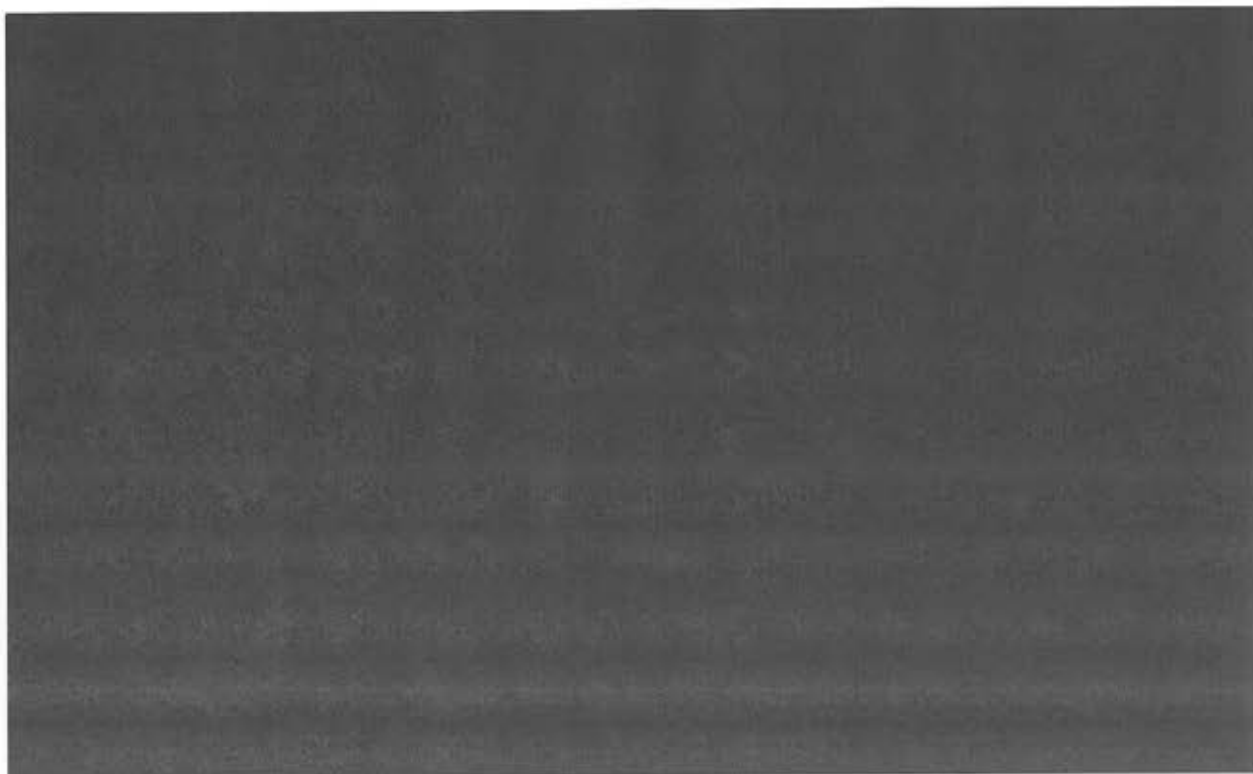
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

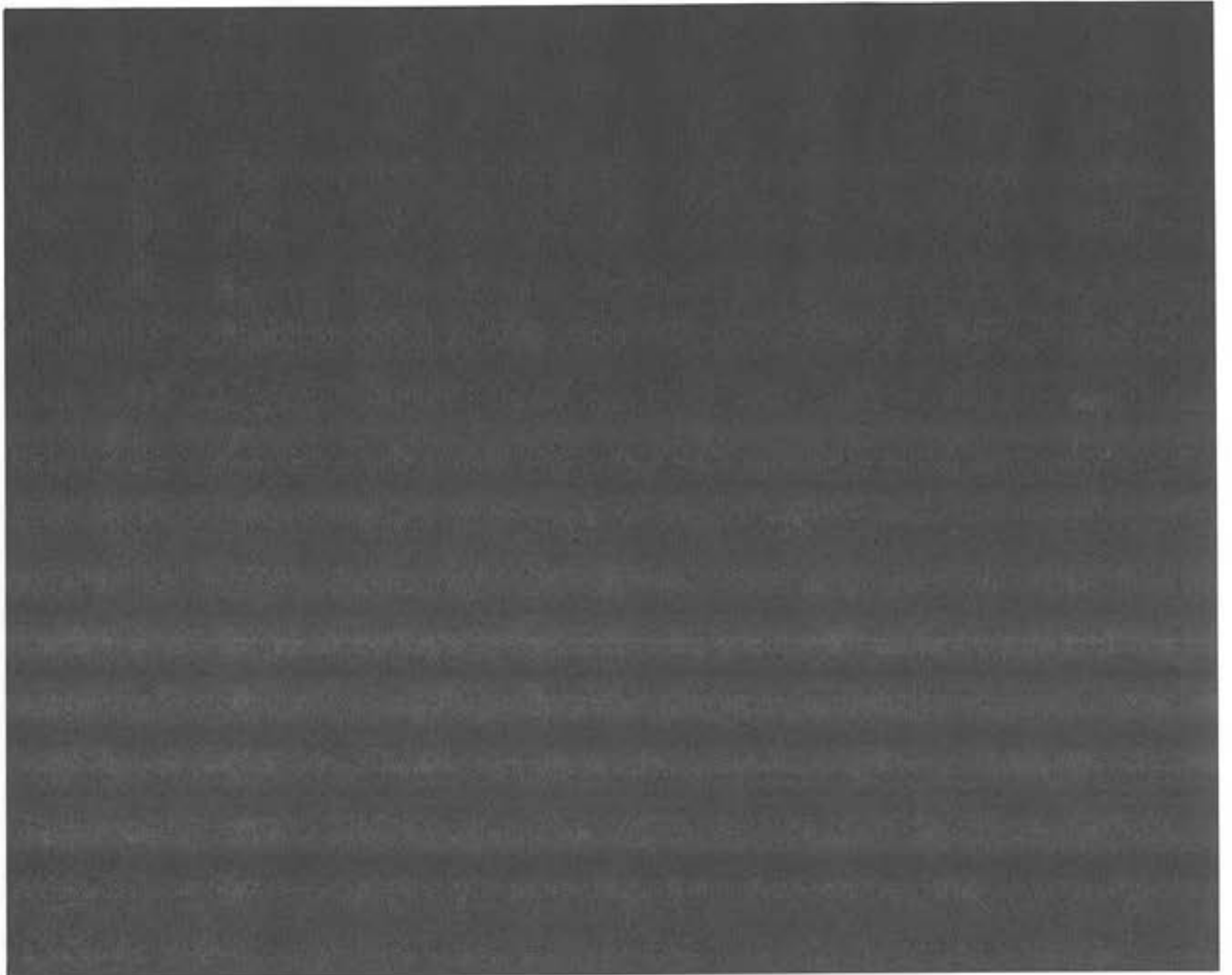
~~TOP SECRET//COMINT//NOFORN//20291123~~



---

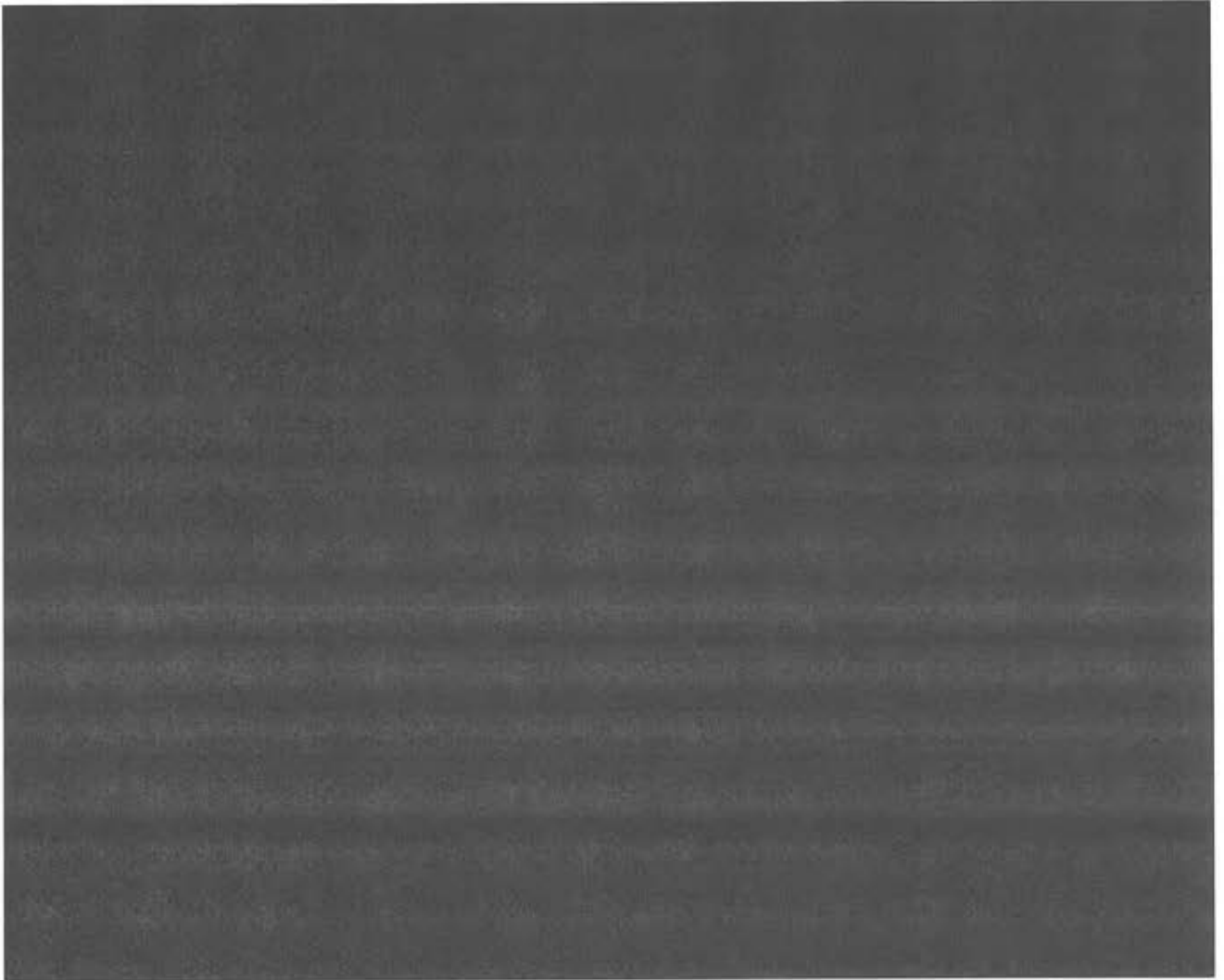
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



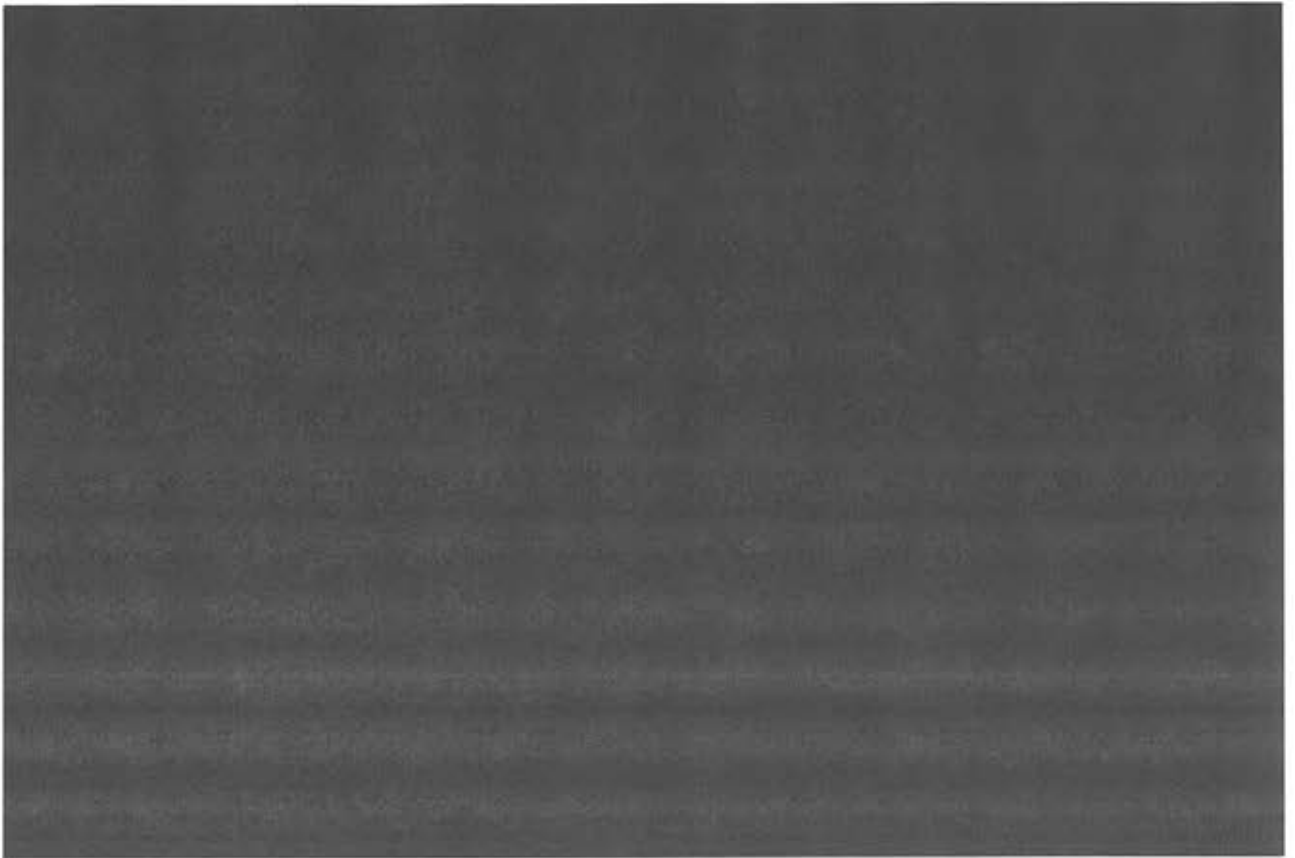
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



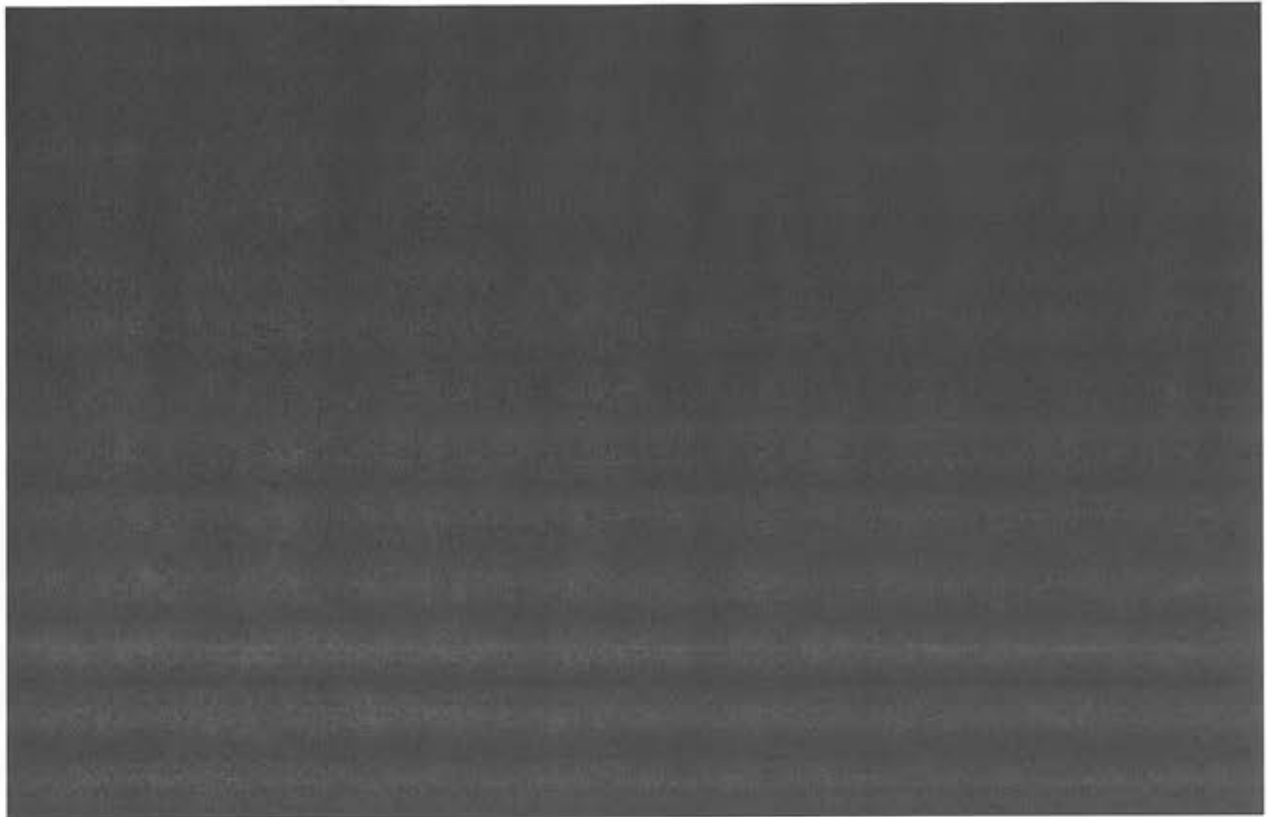
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



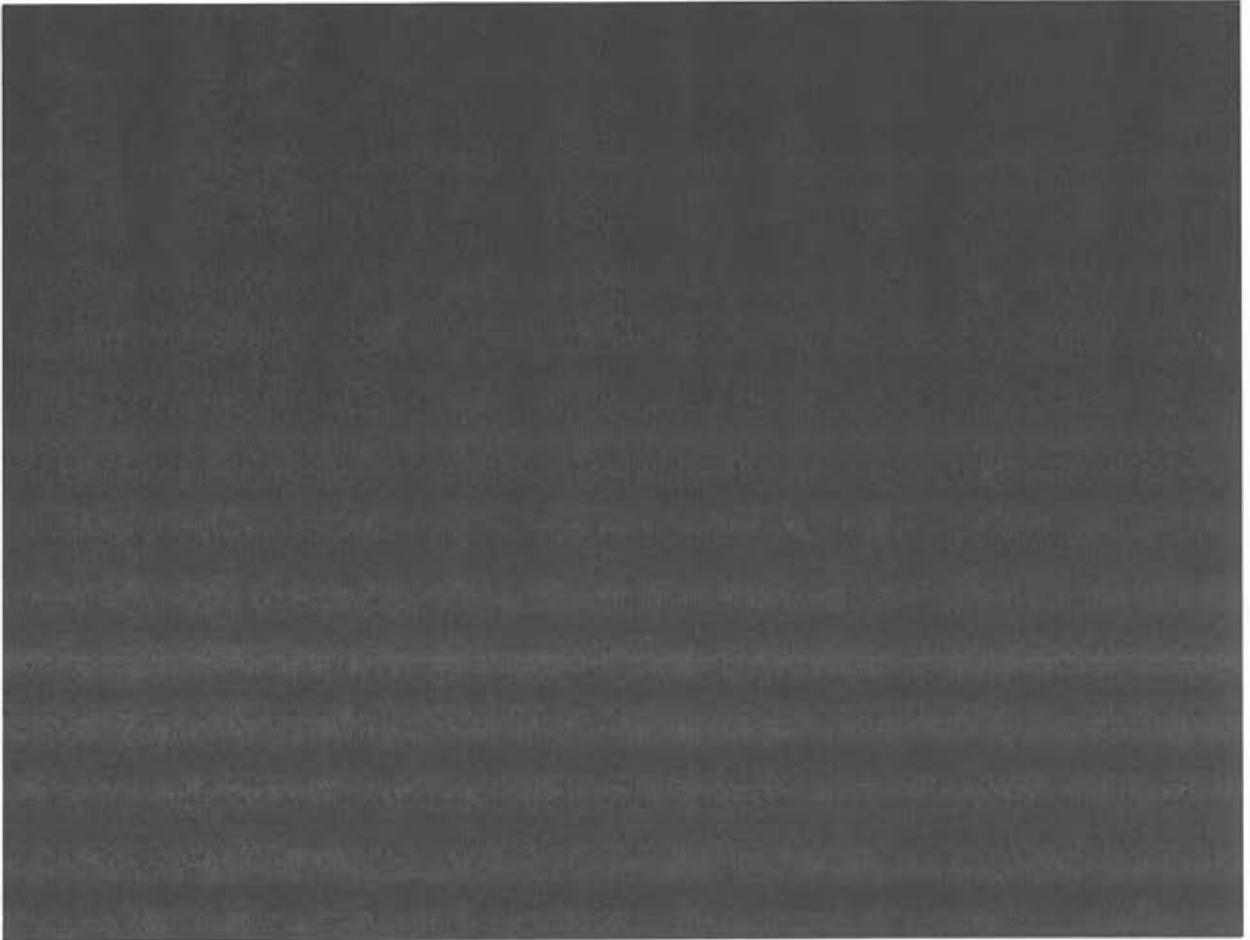
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



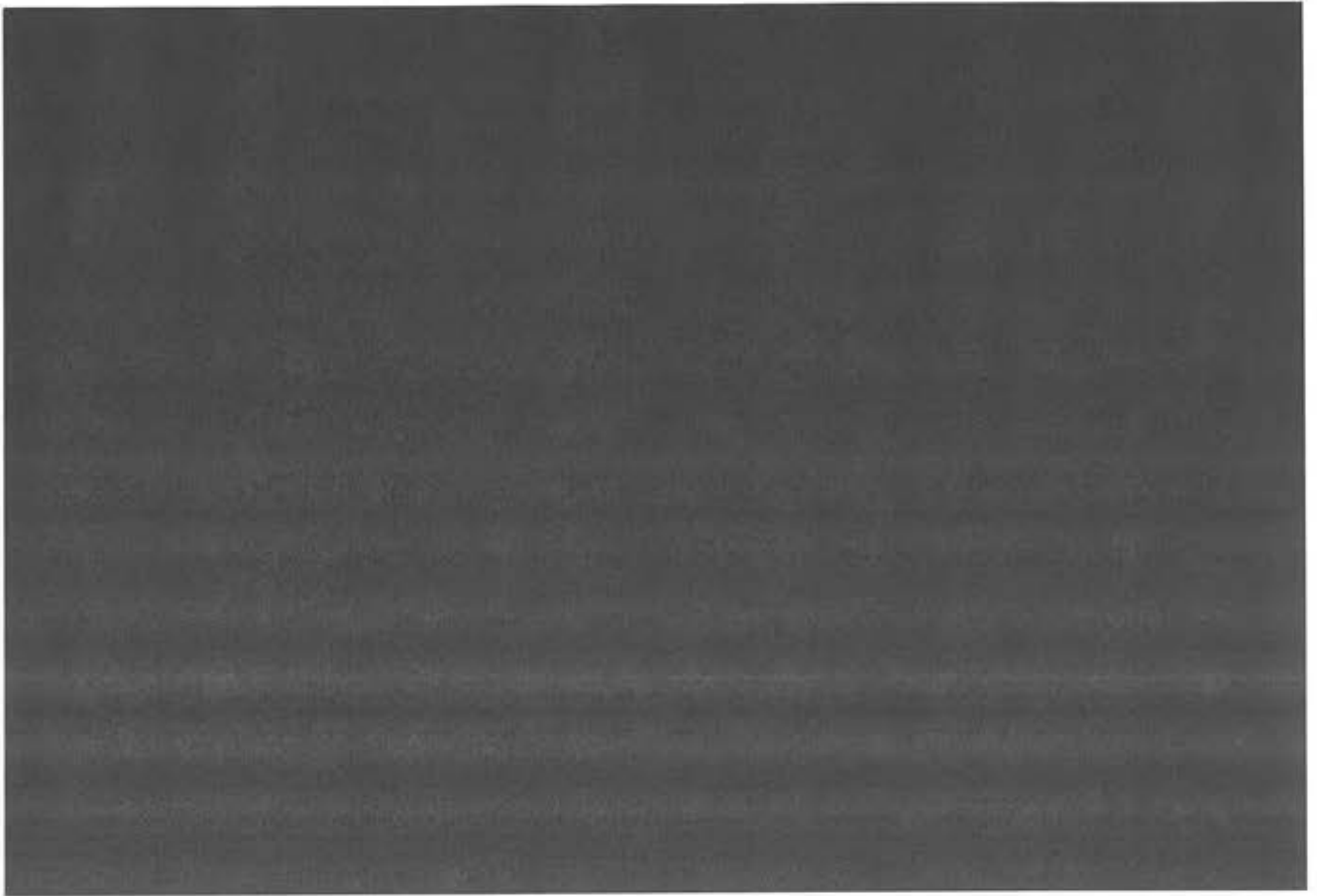
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



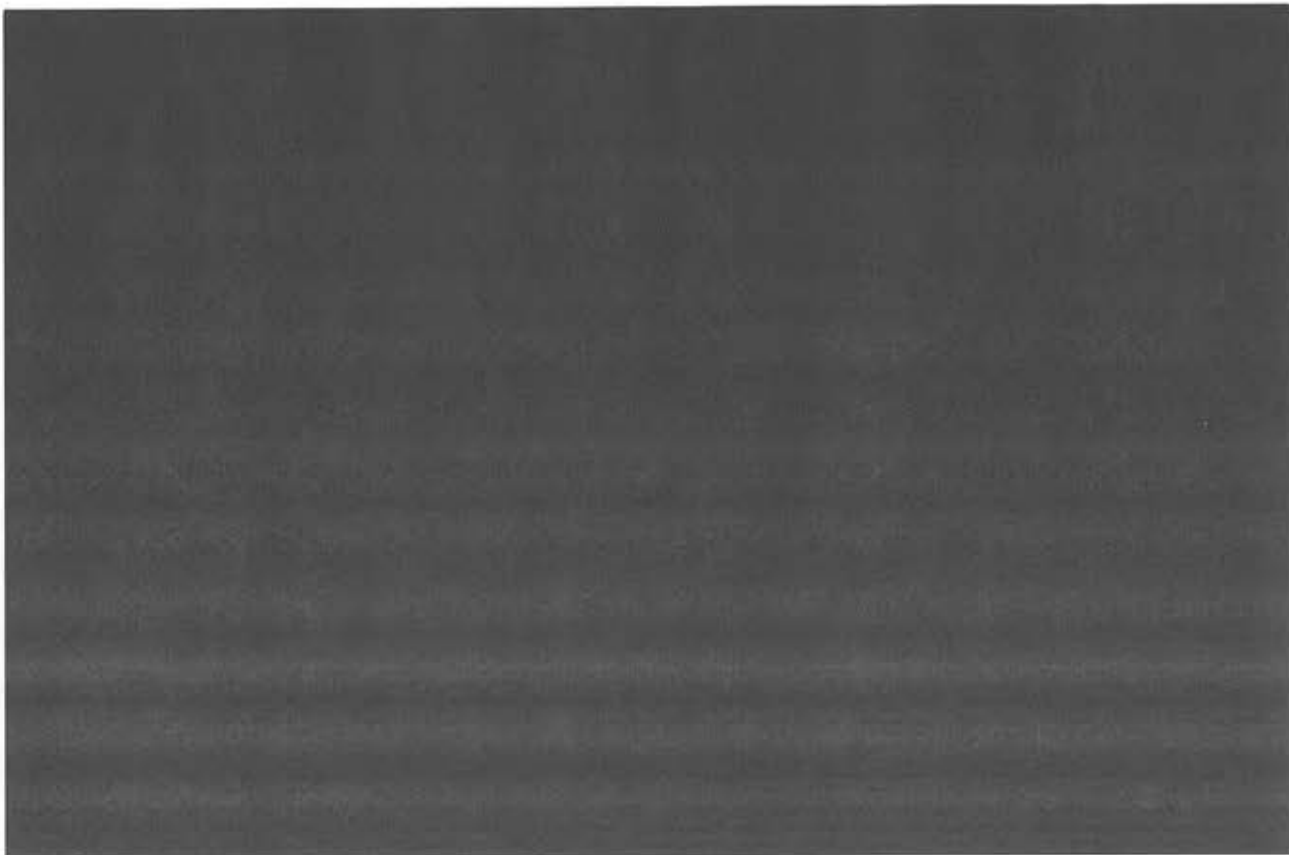
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~

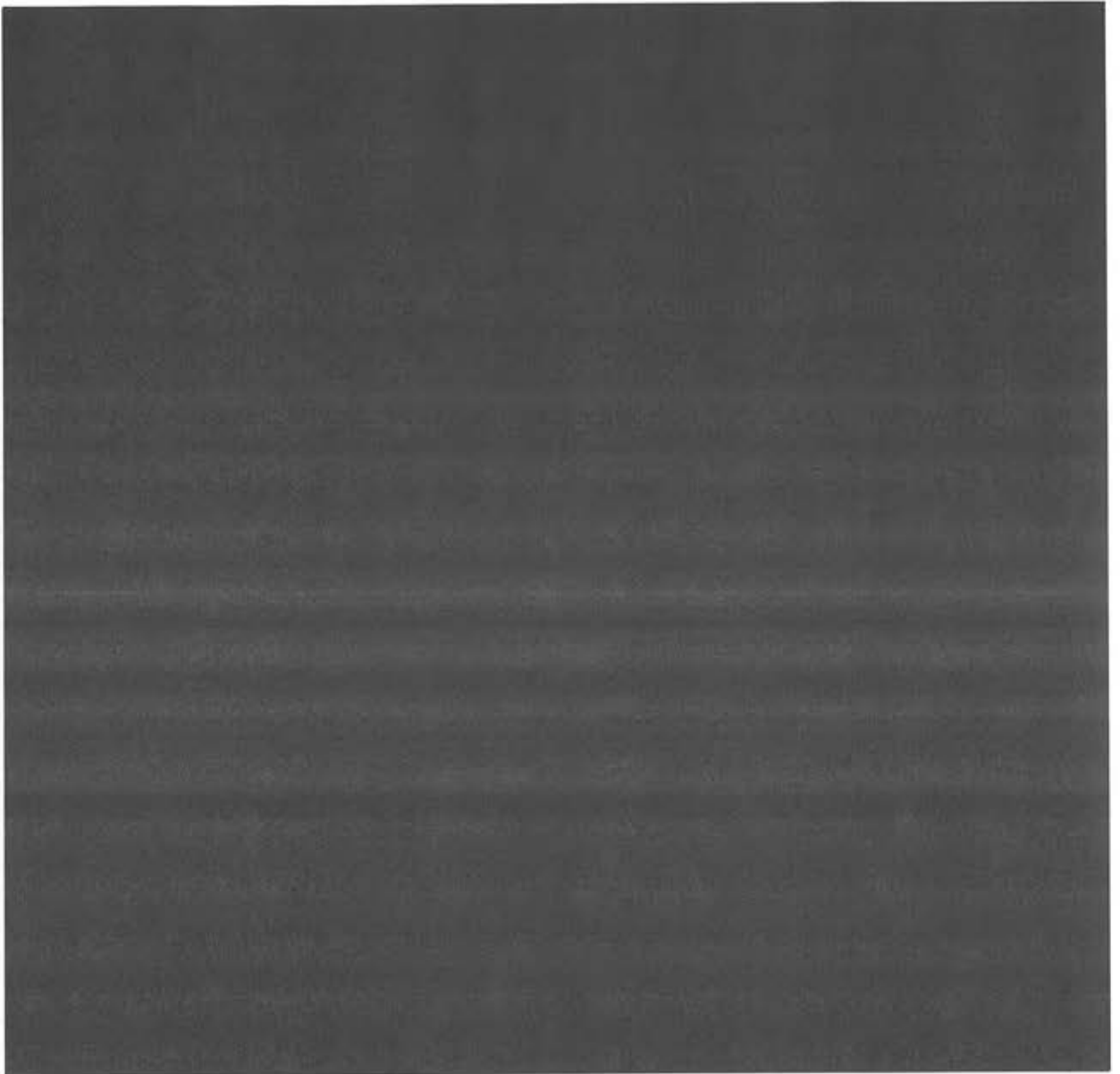
(b)(1); (b)(3); (b)(7)(A)



---

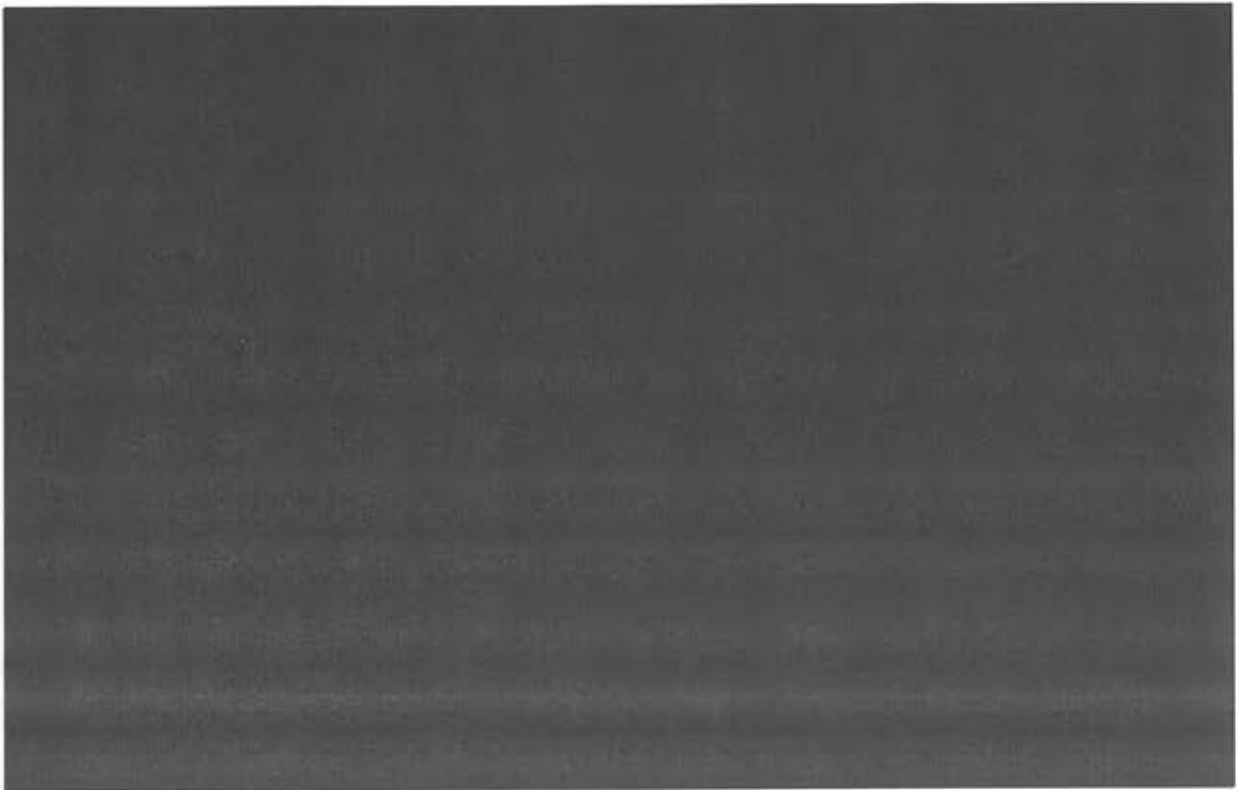
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



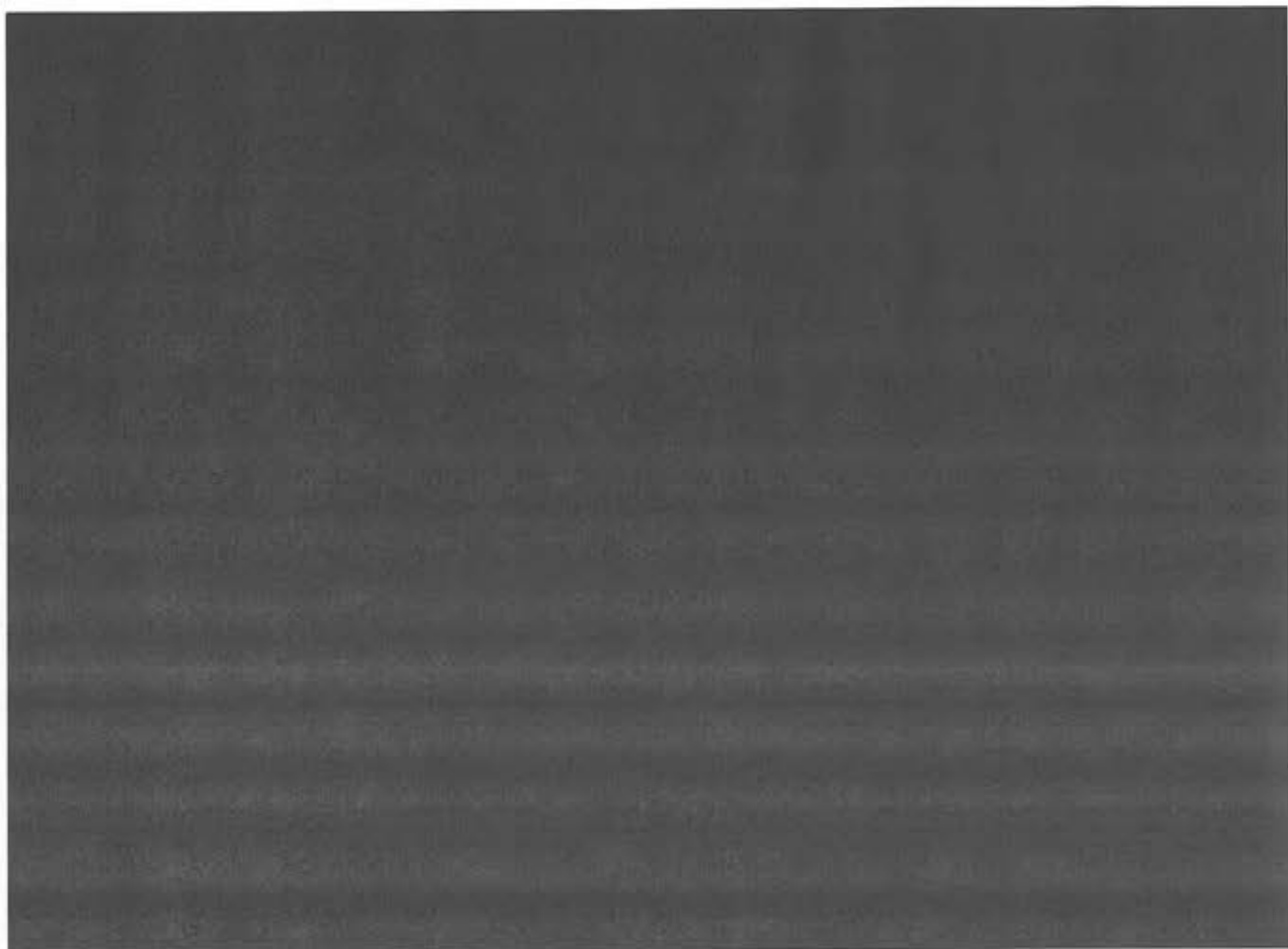
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



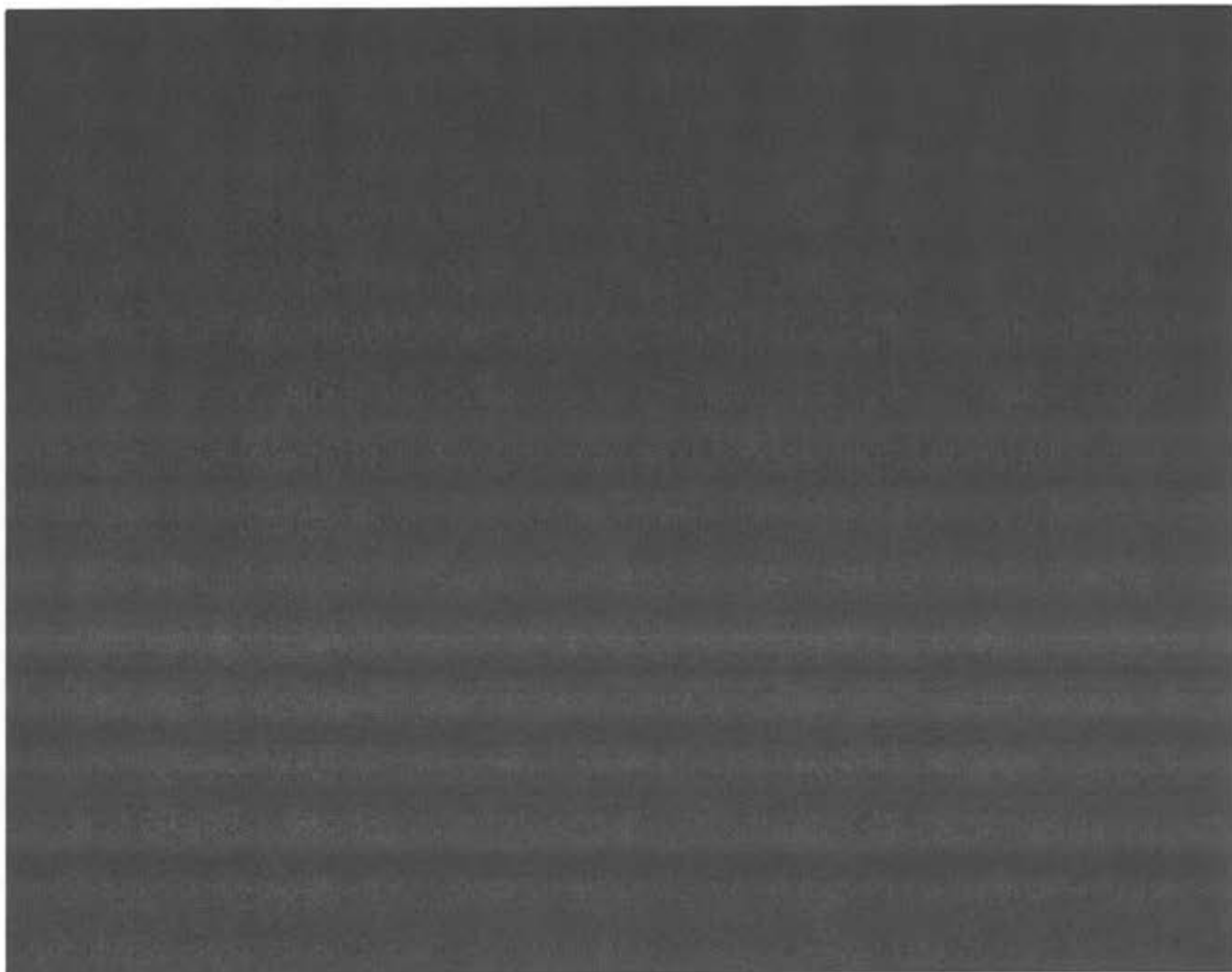
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



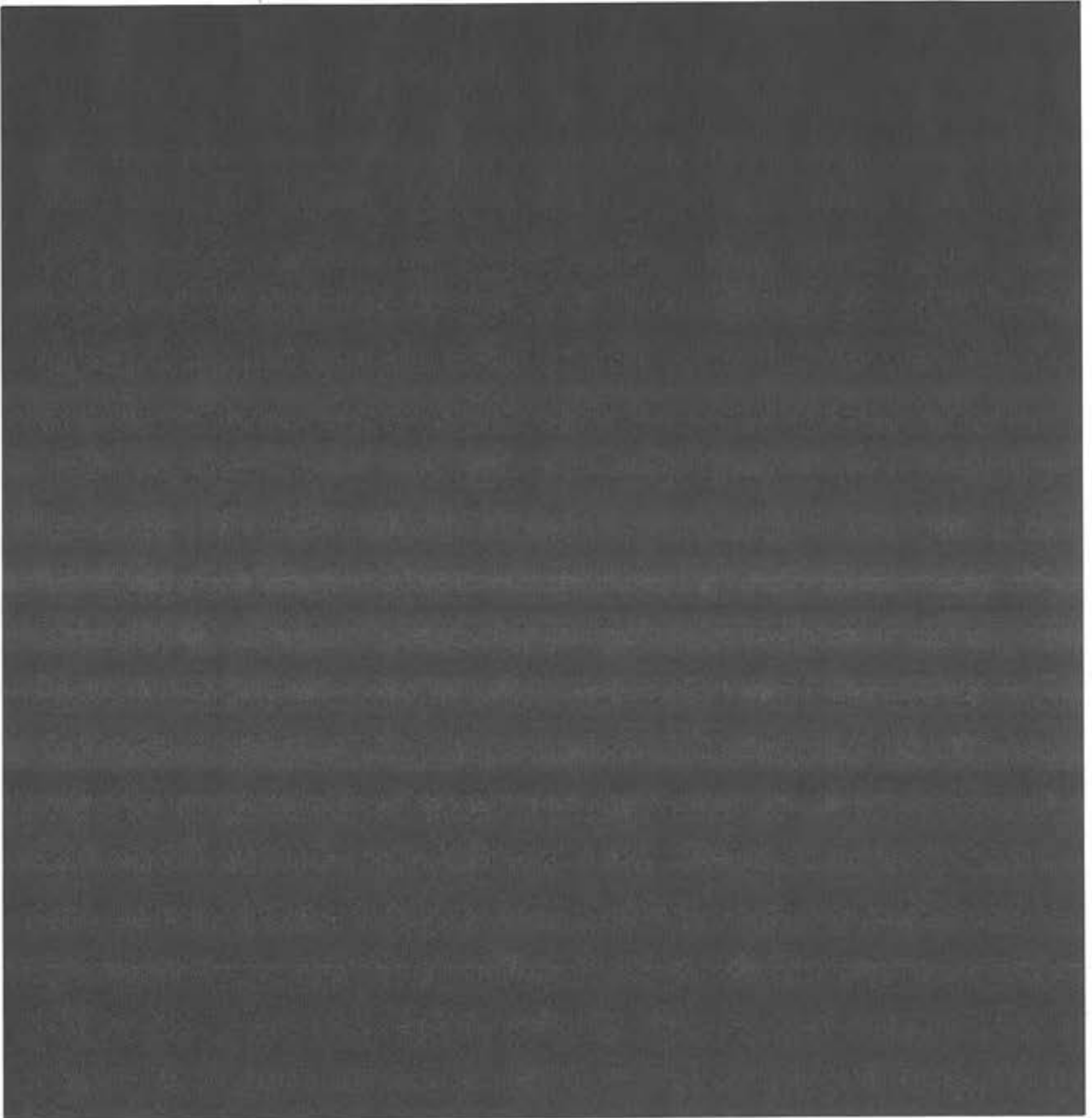
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



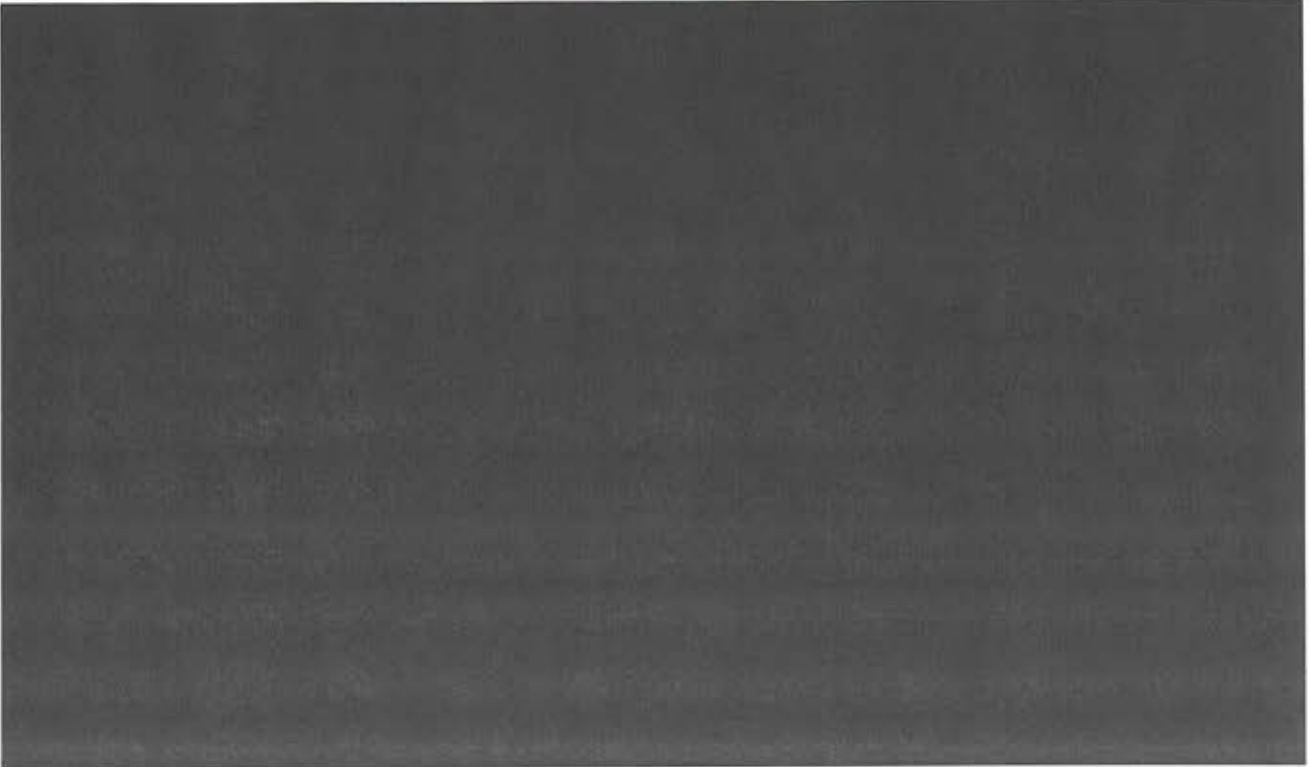
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



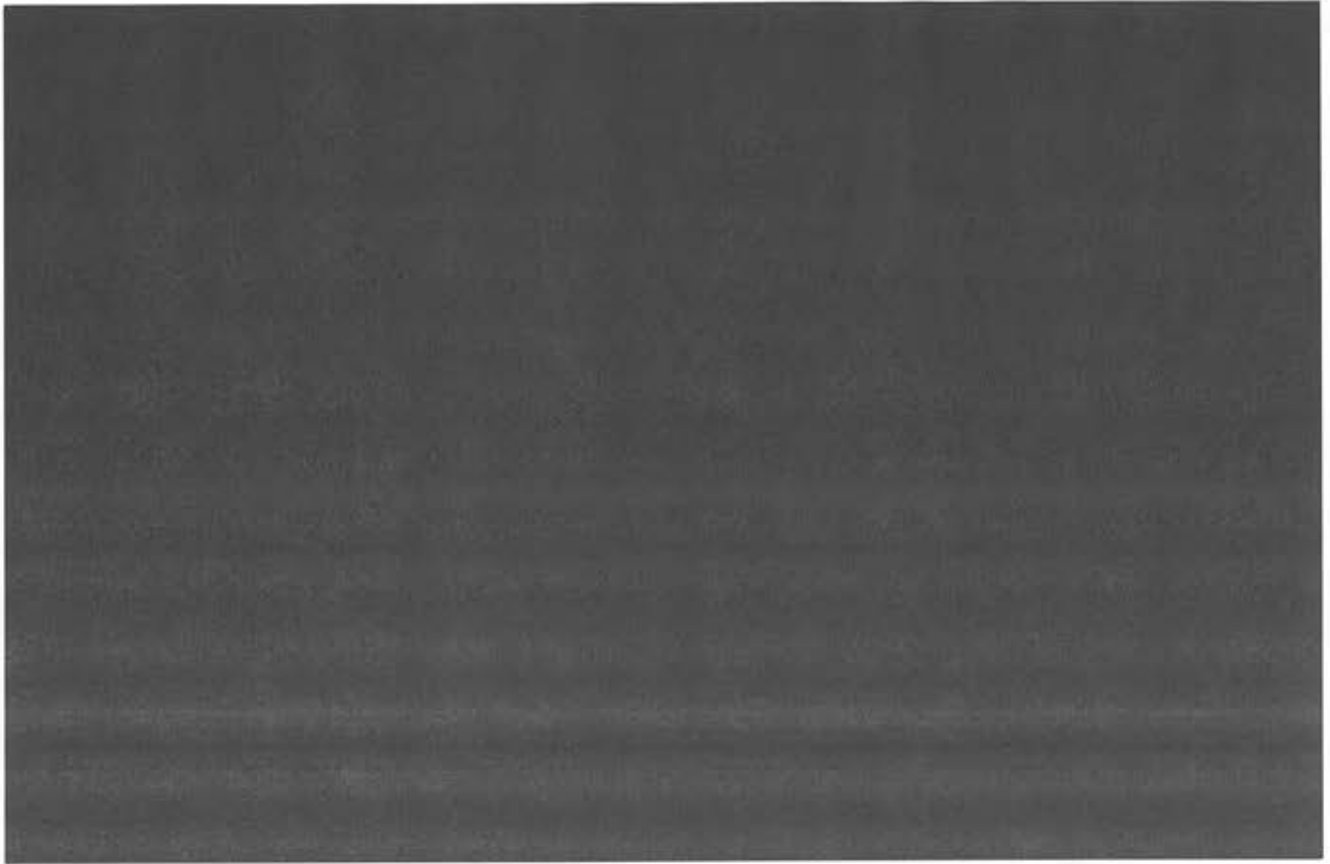
Derived From: NSA/CSSM 1-52

Dated: 20041123

Declassify On: 20291123

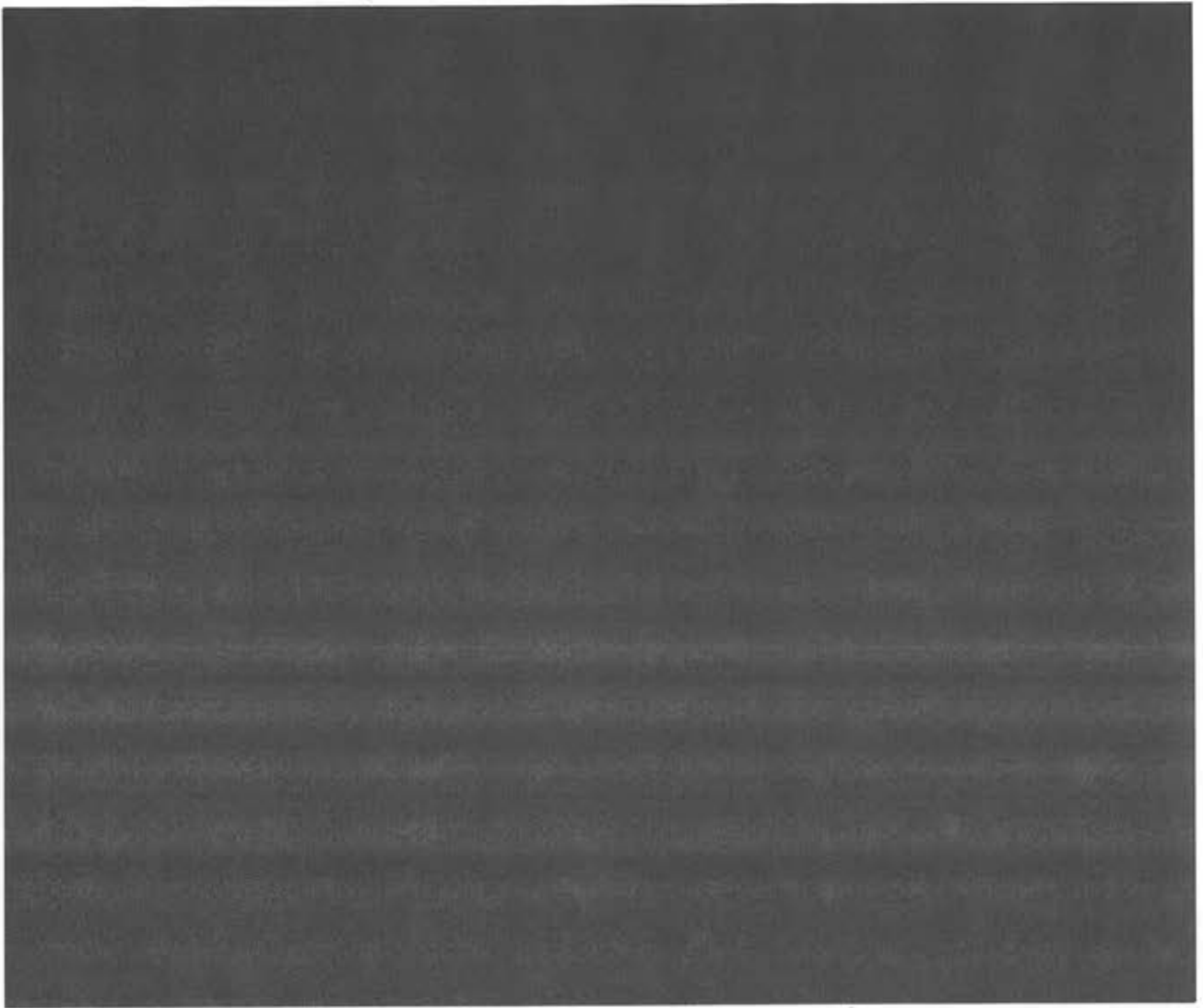
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



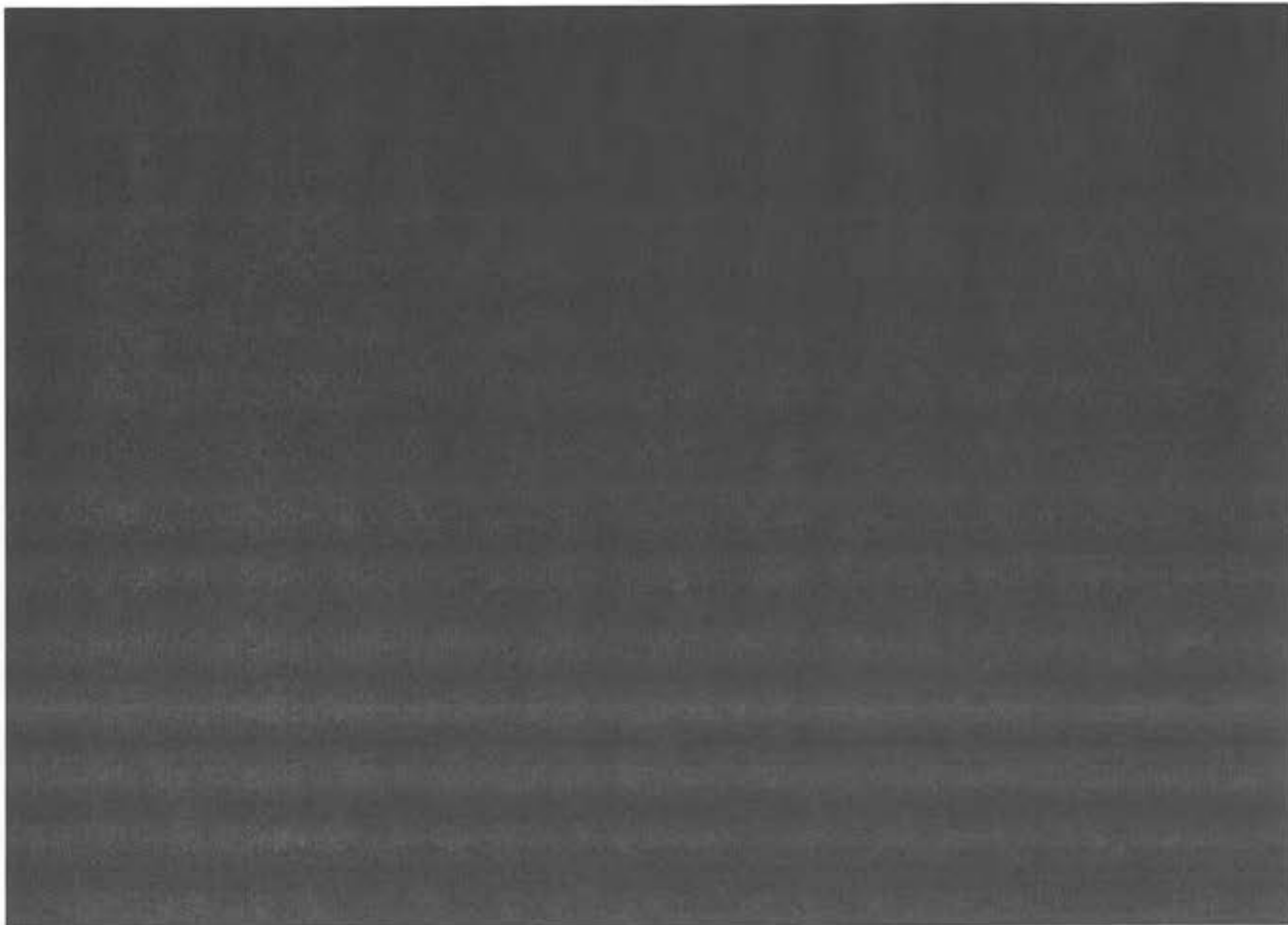
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



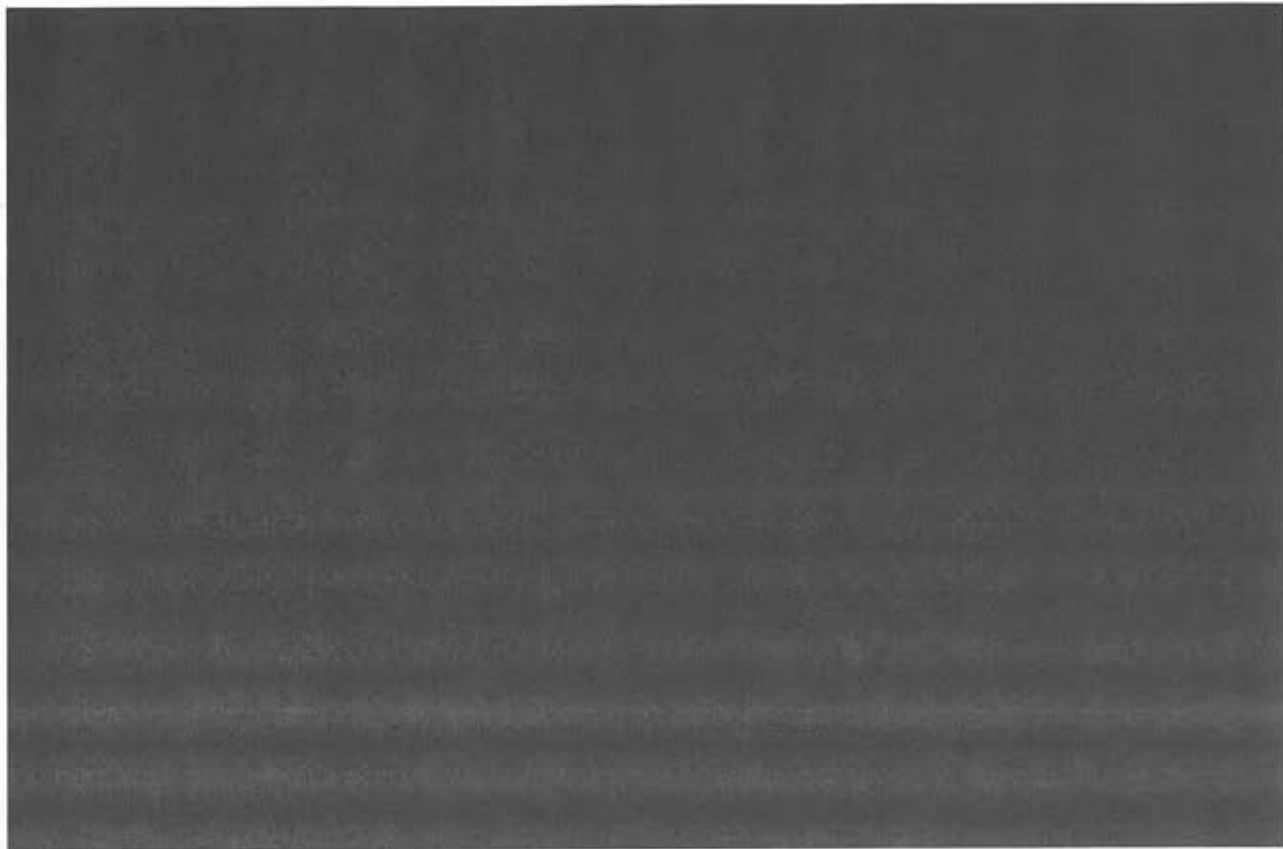
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



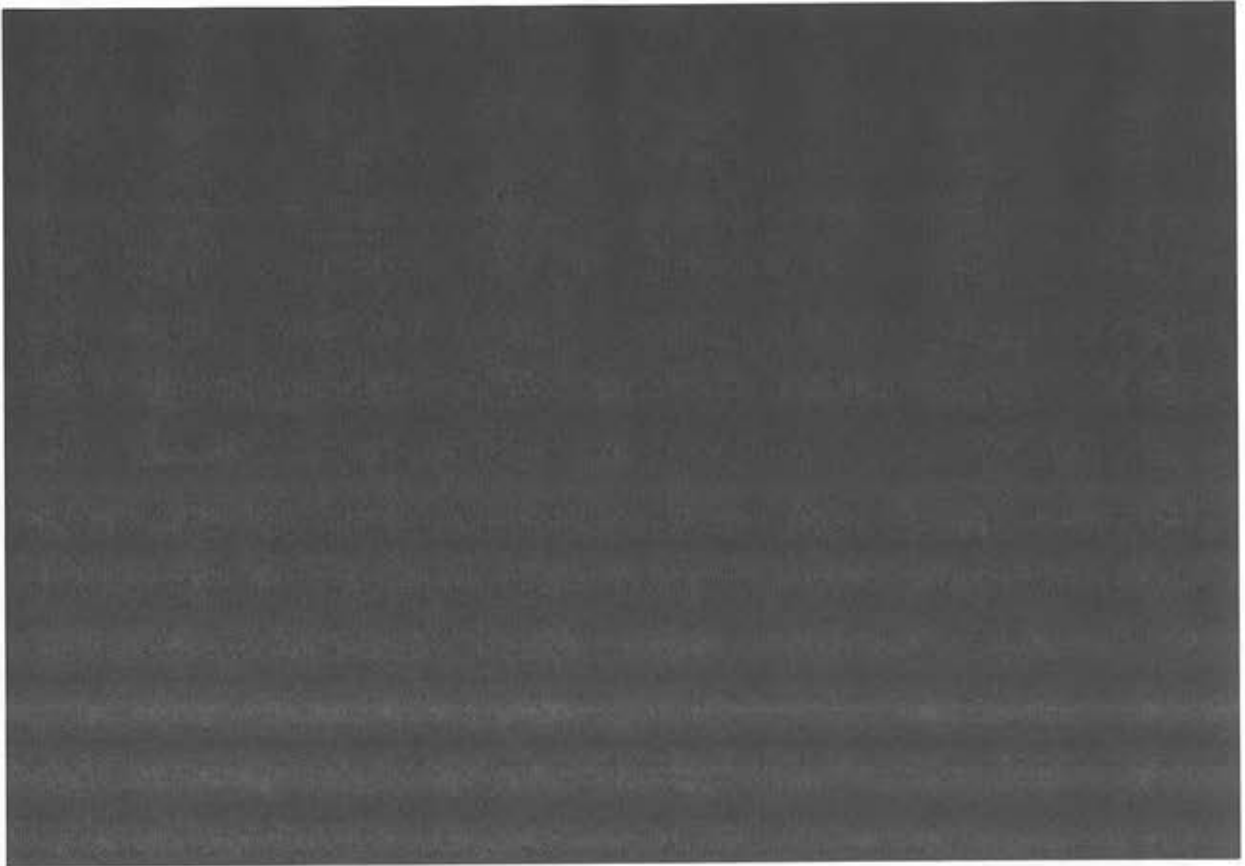
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

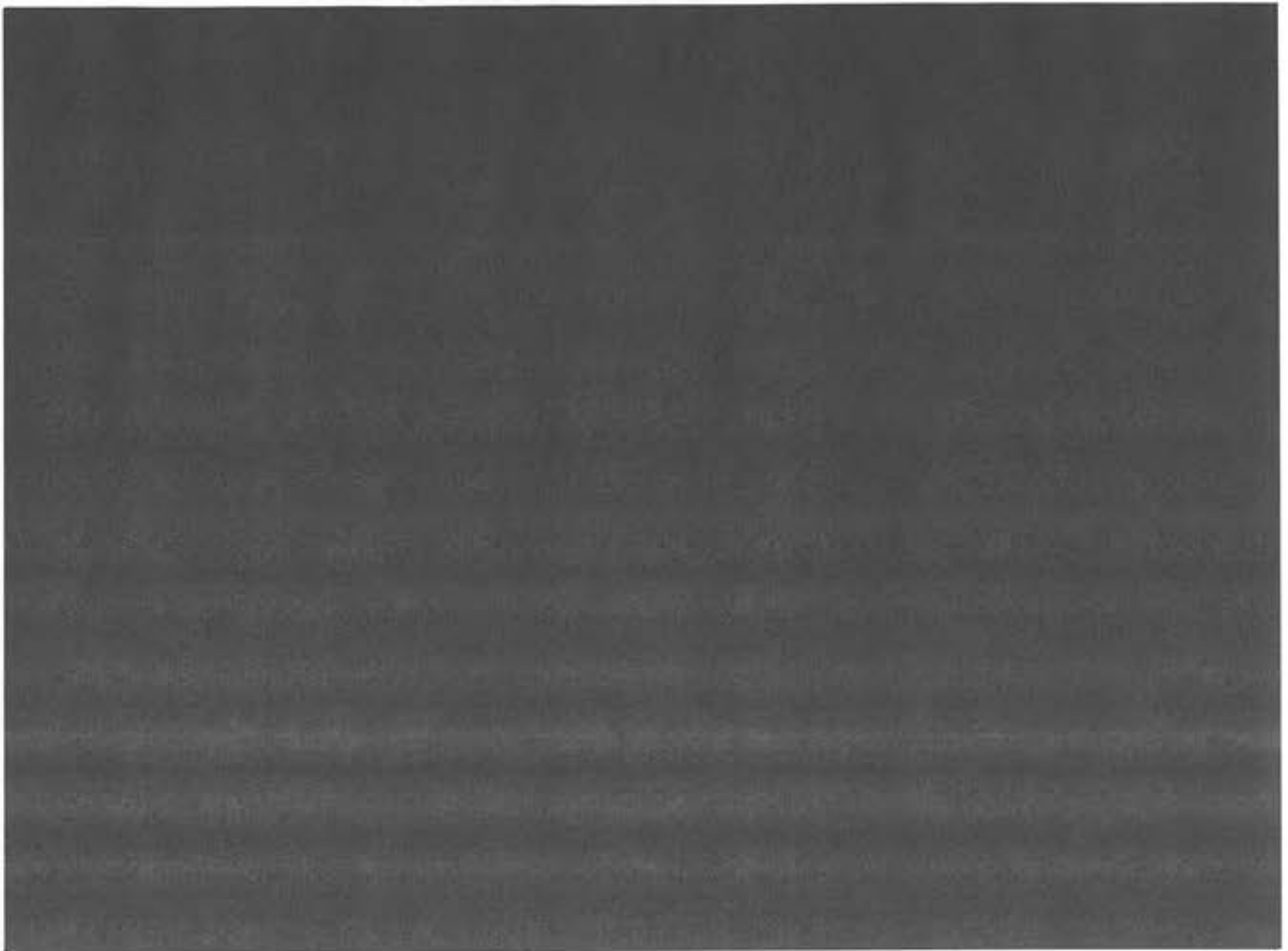
~~TOP SECRET//COMINT//NOFORN//20291123~~



---

~~TOP SECRET//COMINT//NOFORN//20291123~~

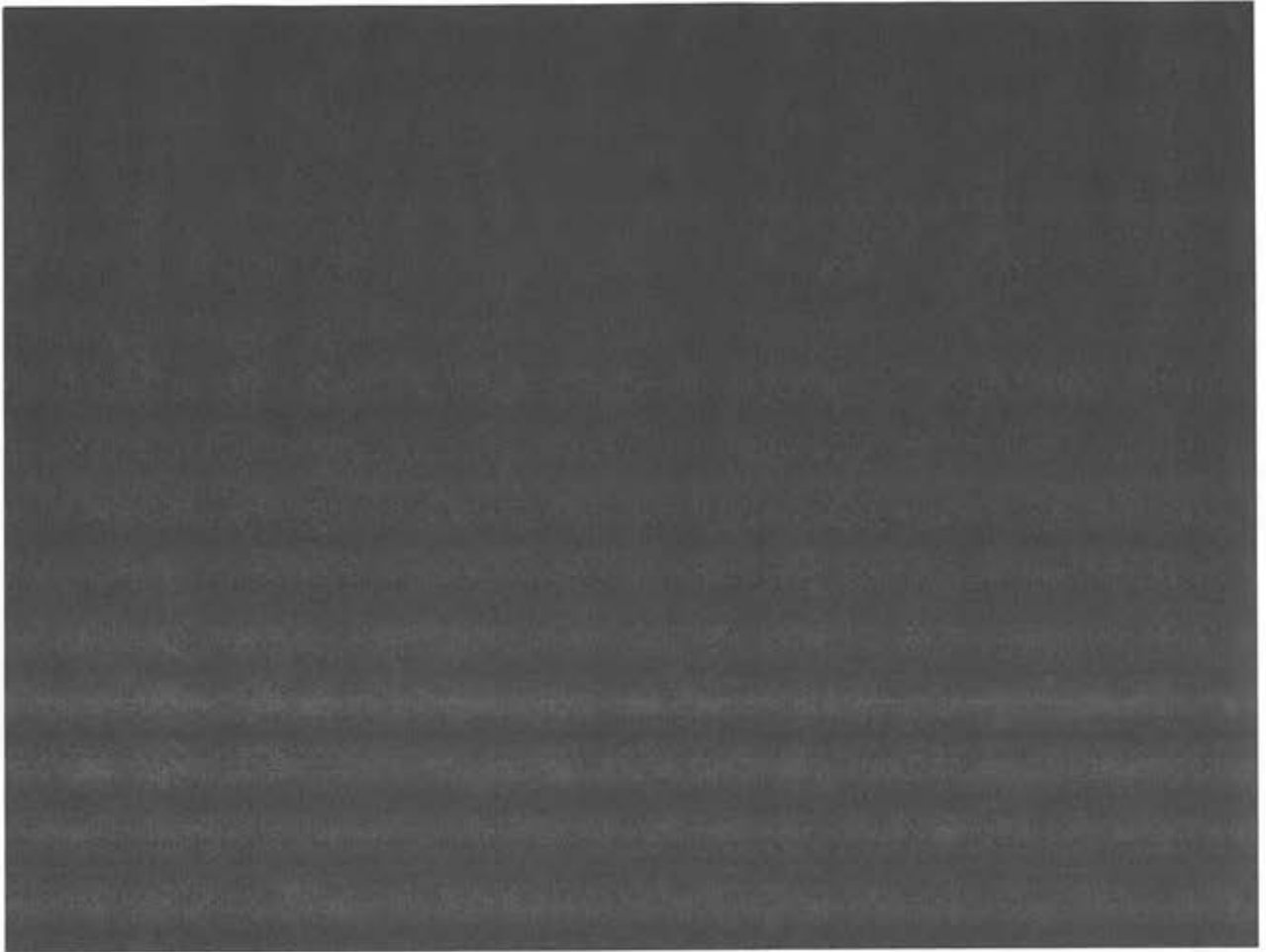
~~TOP SECRET//COMINT//NOFORN//20291123~~



---

~~TOP SECRET//COMINT//NOFORN//20291123~~

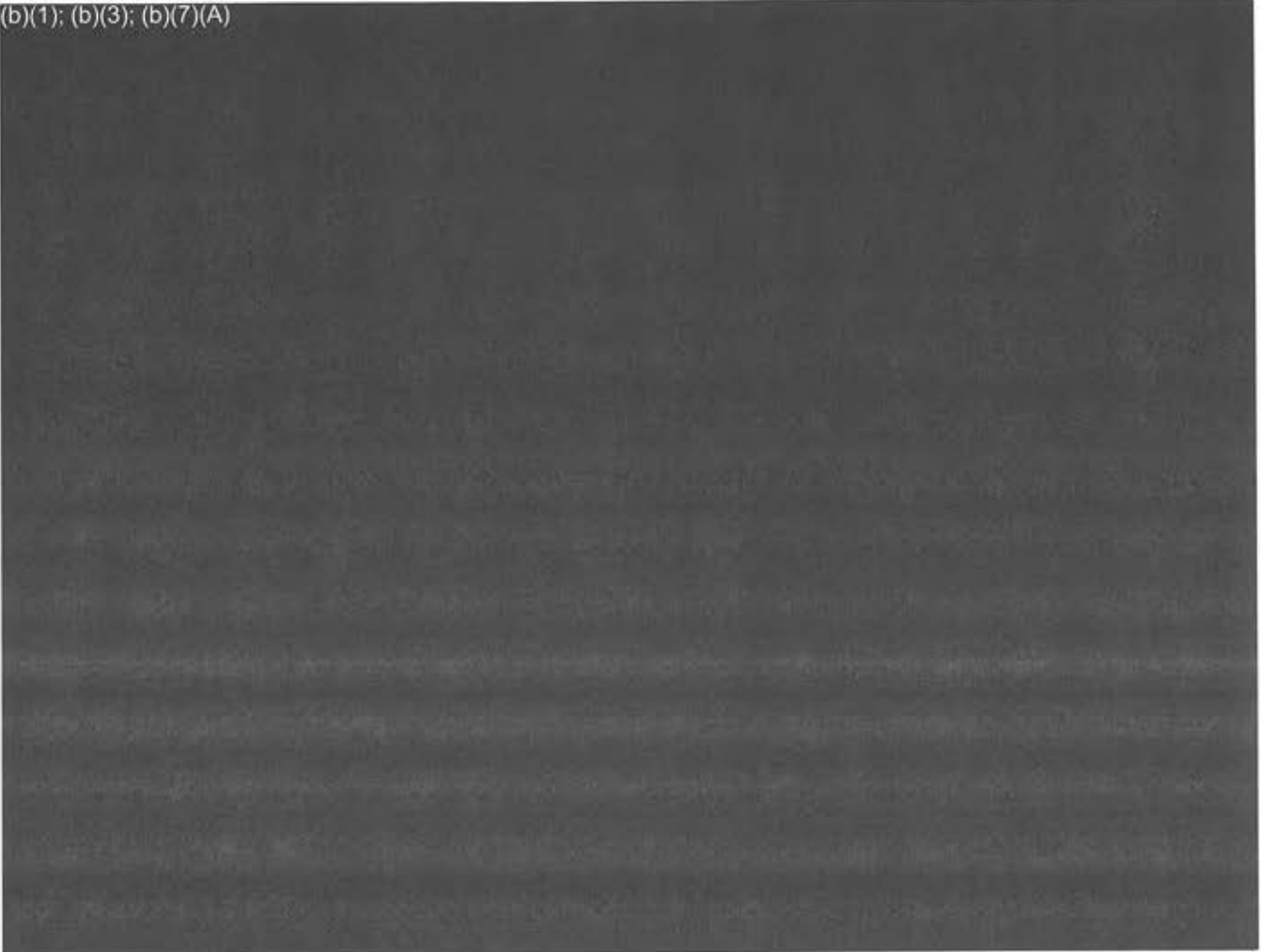
~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~

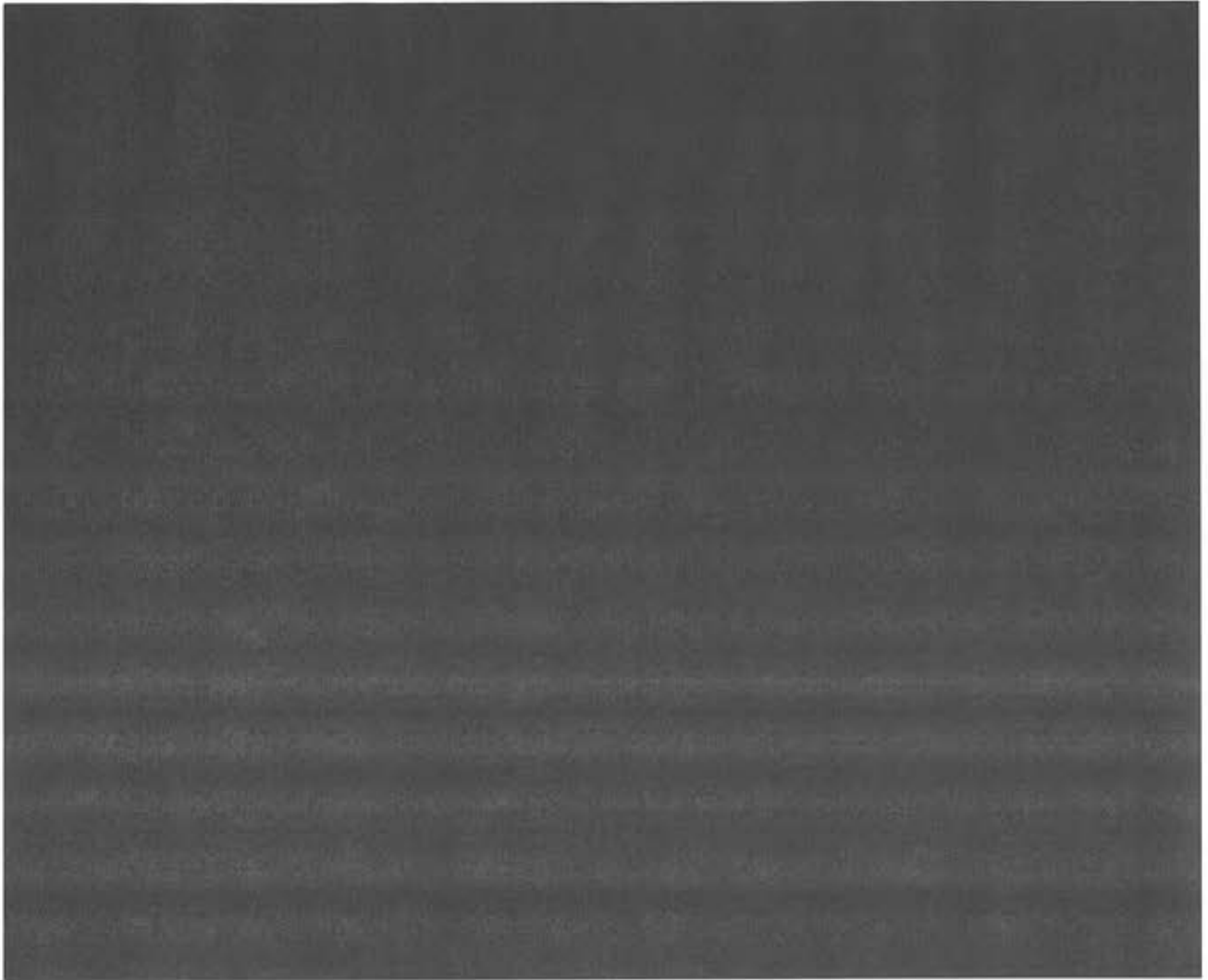
(b)(1); (b)(3); (b)(7)(A)



---

~~TOP SECRET//COMINT//NOFORN//20291123~~

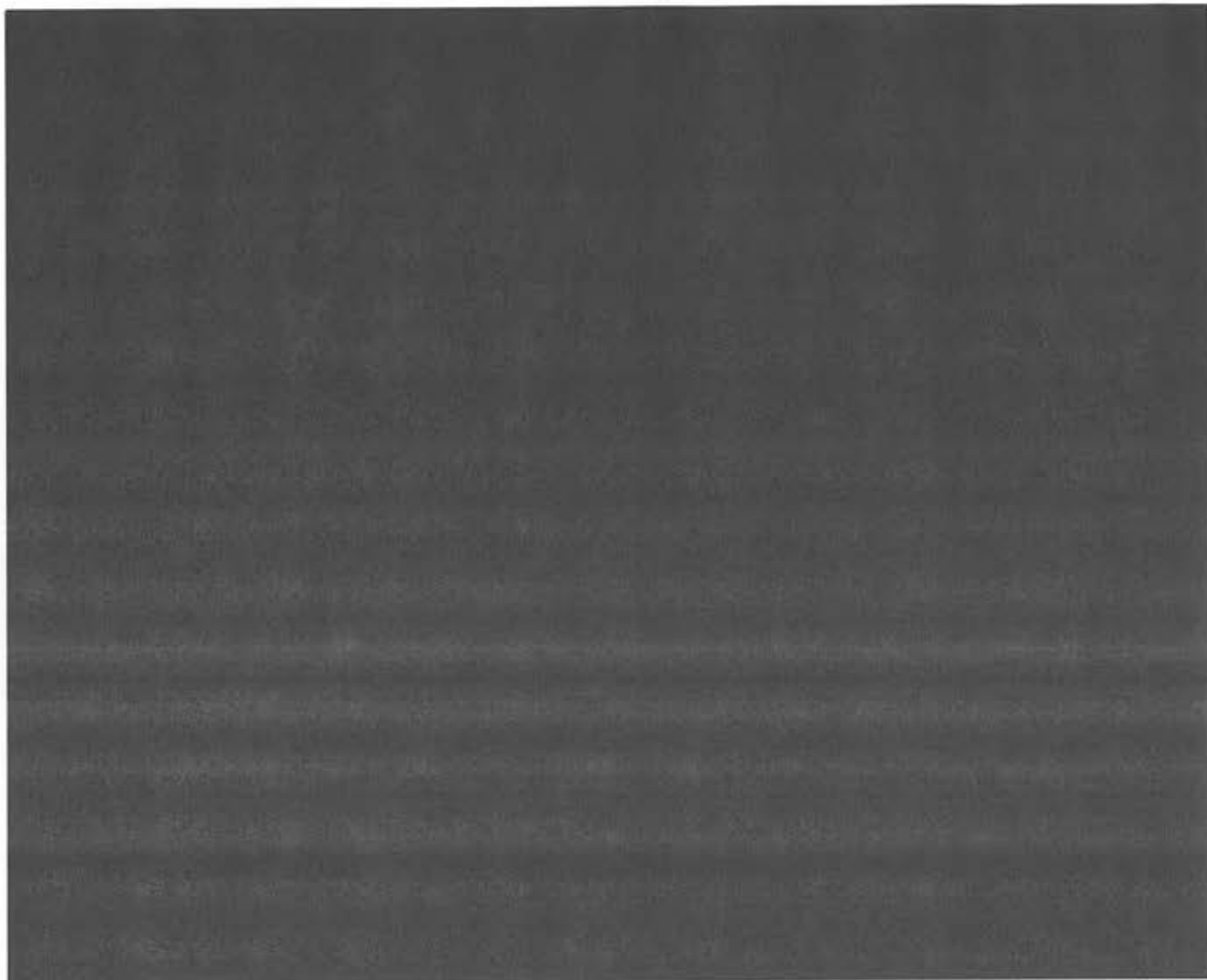
~~TOP SECRET//COMINT//NOFORN//20291123~~



---

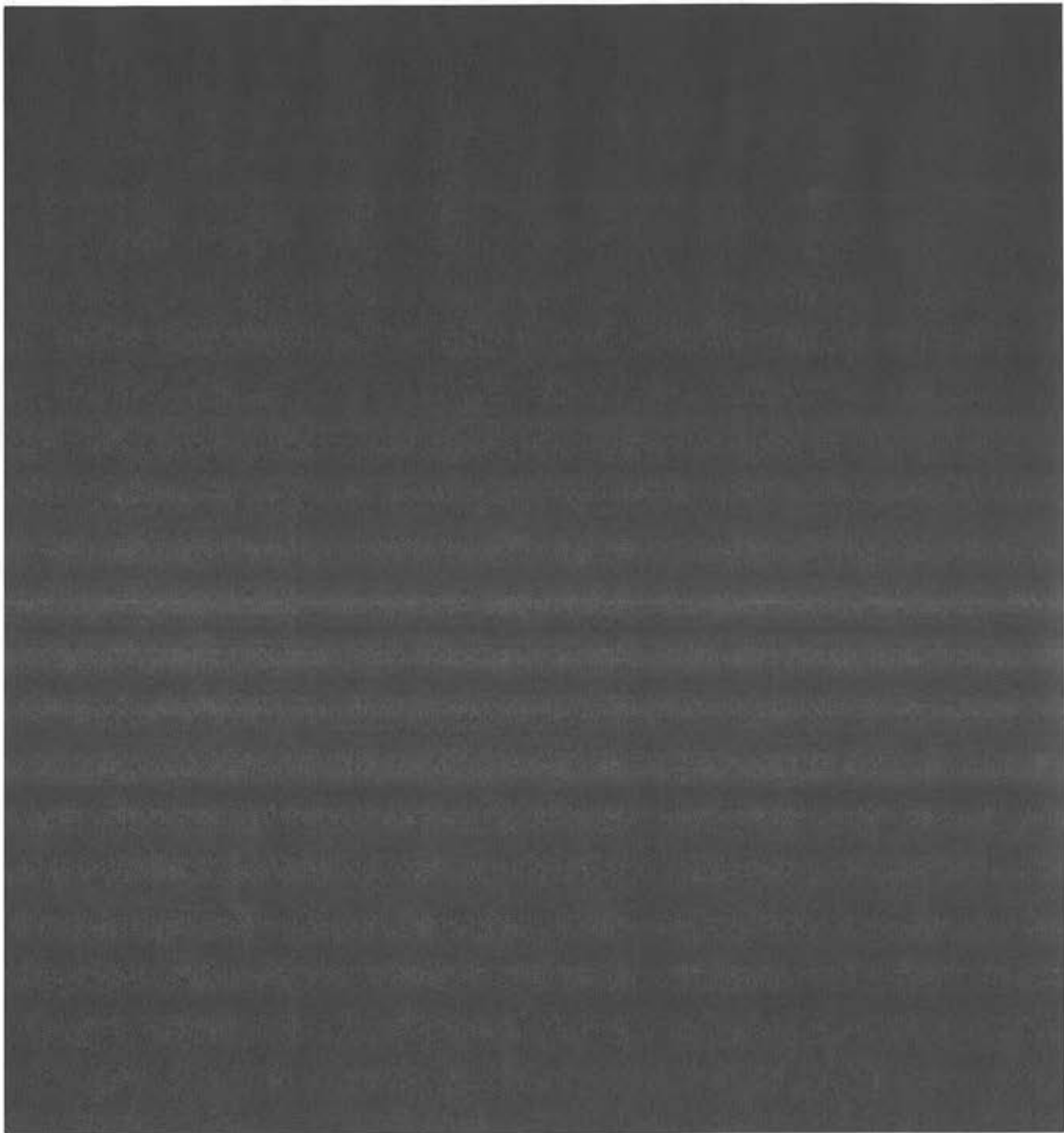
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



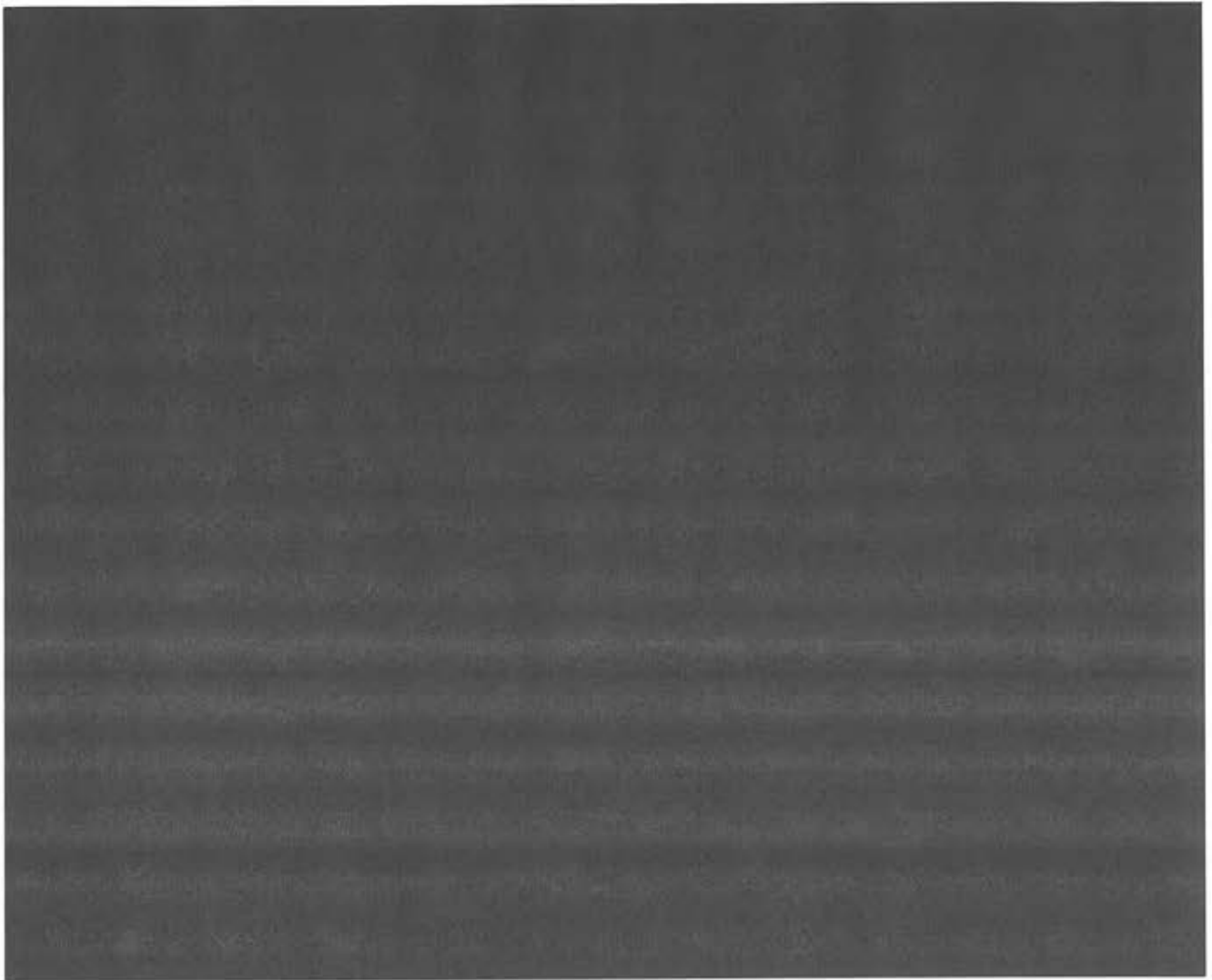
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



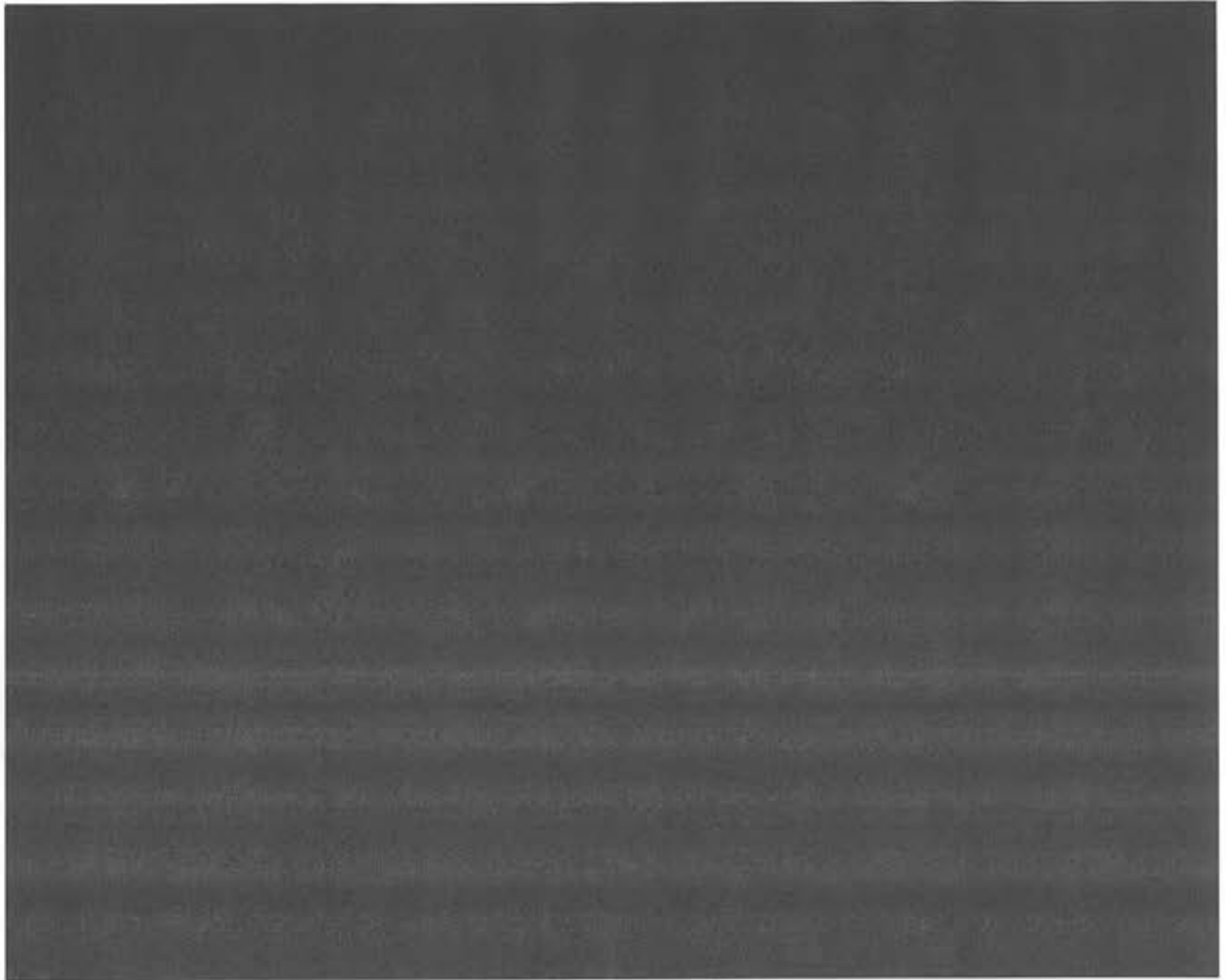
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~

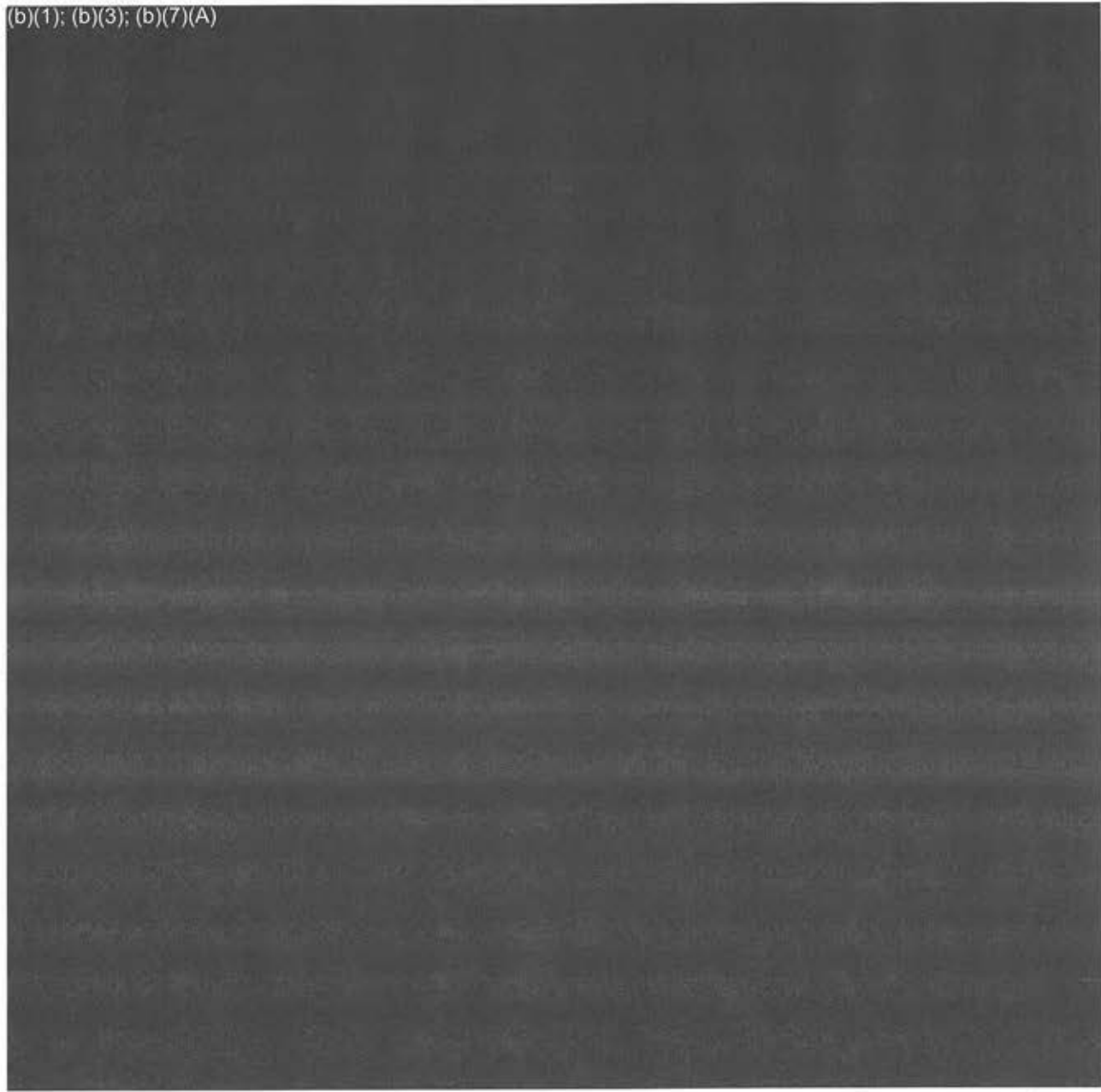


---

~~TOP SECRET//COMINT//NOFORN//20291123~~

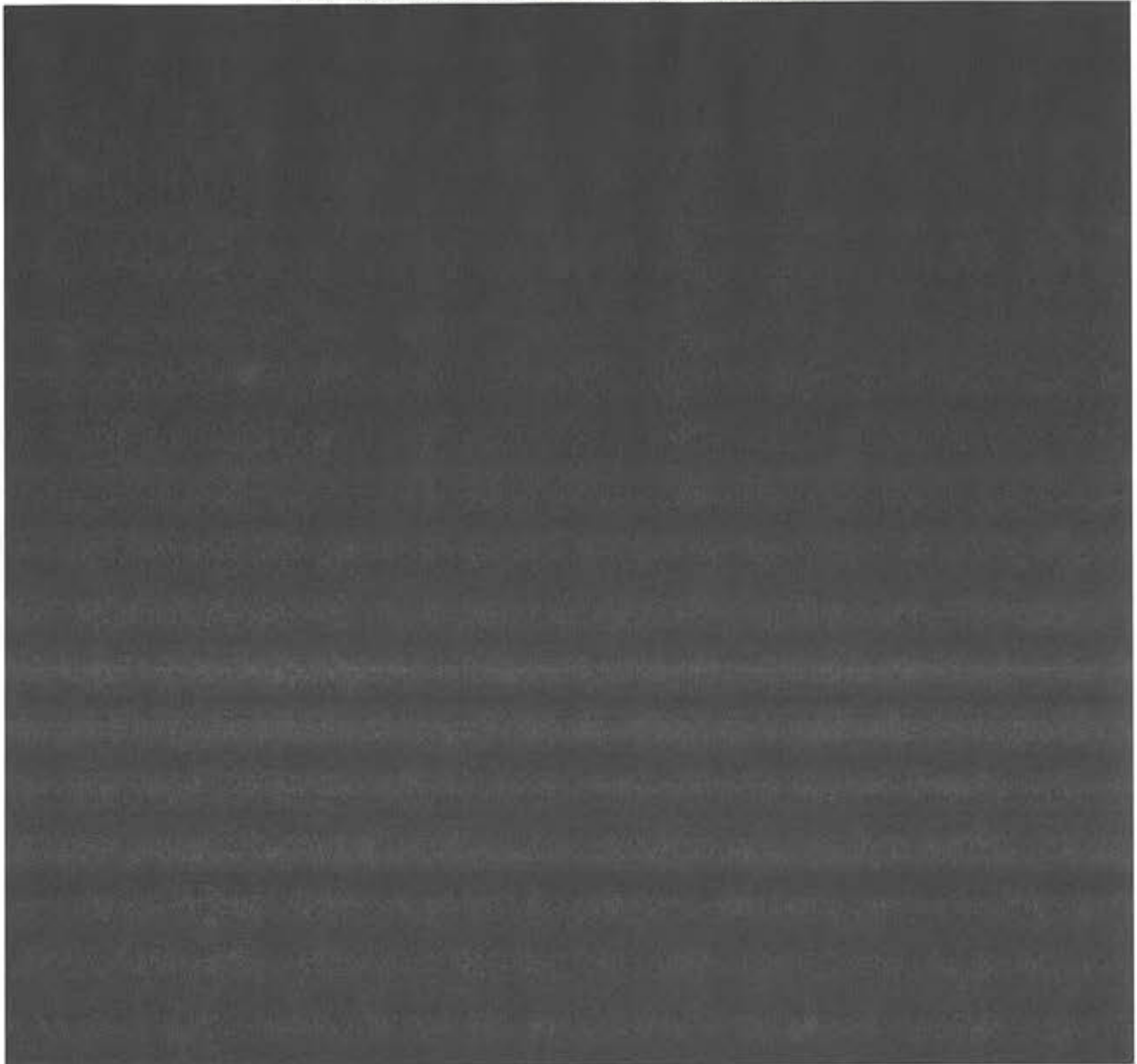
~~TOP SECRET//COMINT//NOFORN//20291123~~

(b)(1); (b)(3); (b)(7)(A)



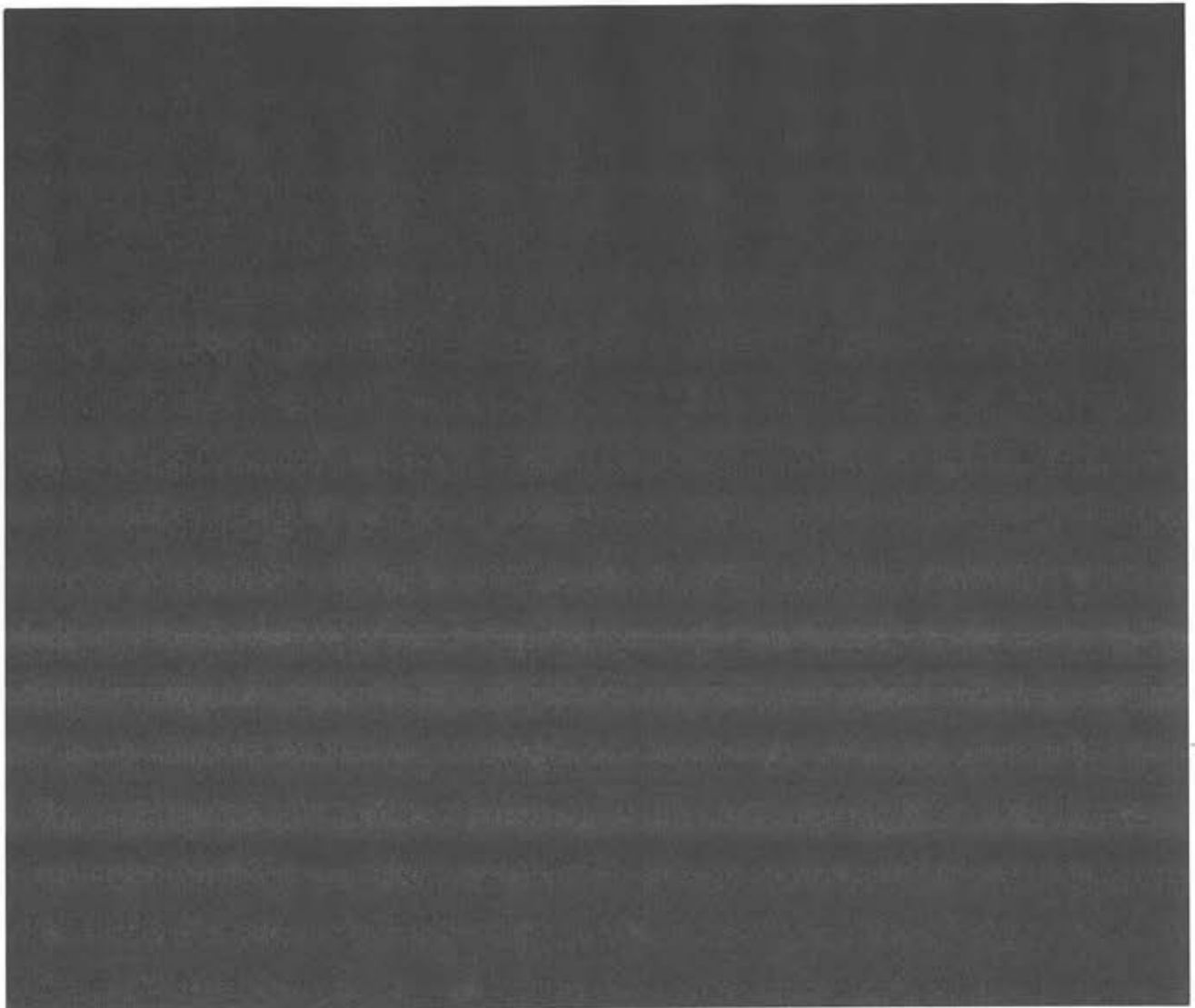
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



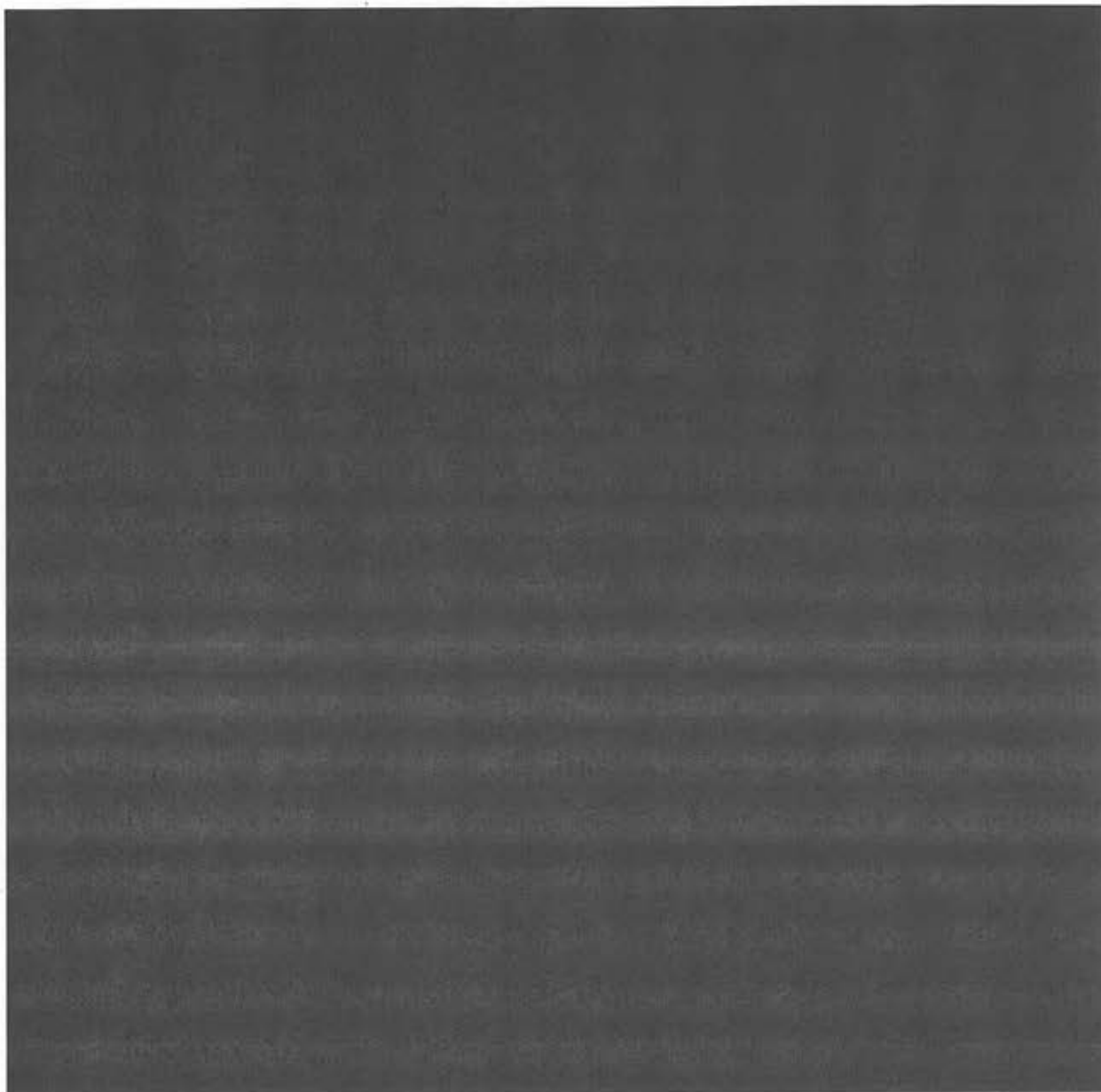
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

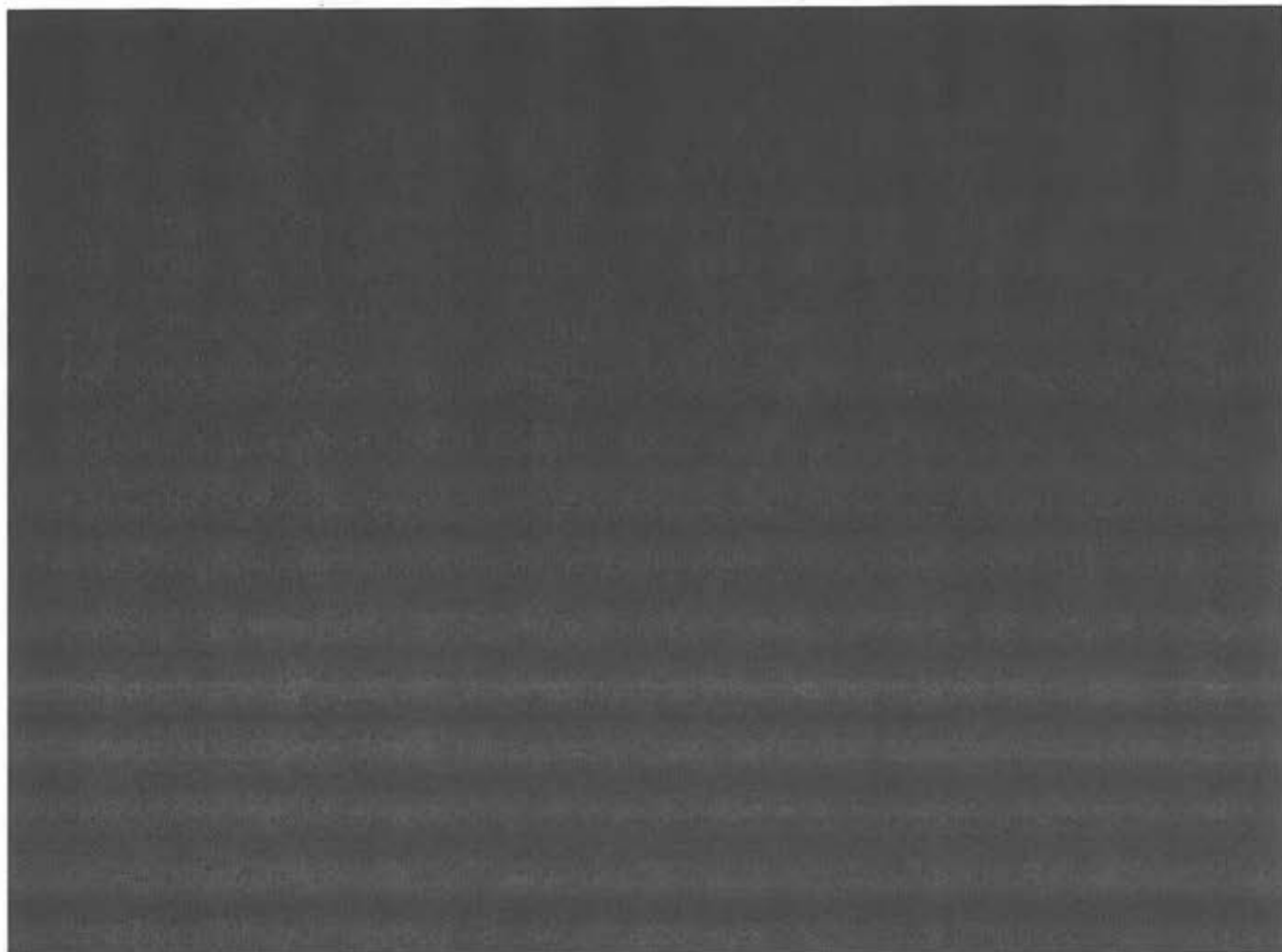
TOP SECRET//COMINT//NOFORN//20291123



---

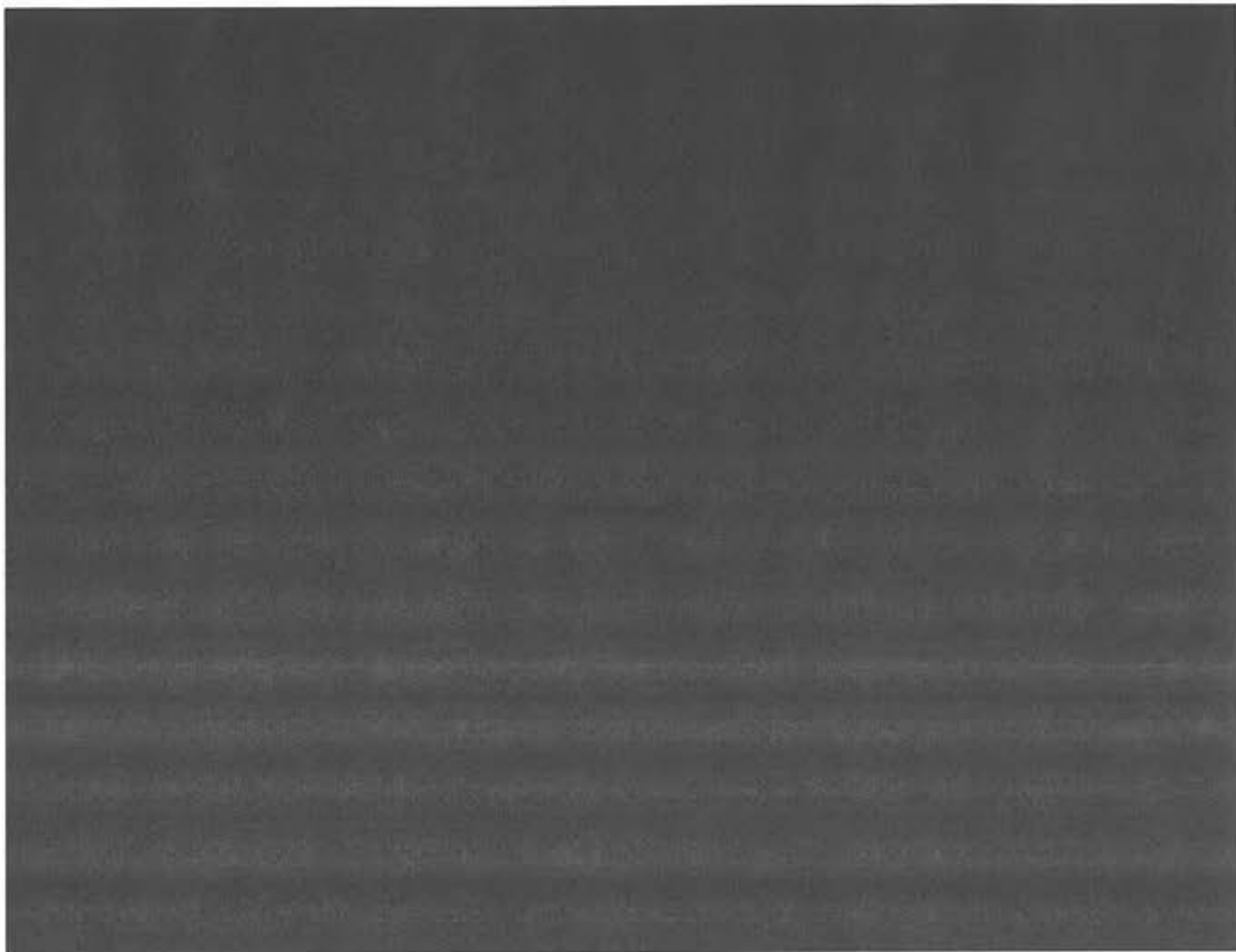
TOP SECRET//COMINT//NOFORN//20291123

~~TOP SECRET//COMINT//NOFORN//20291123~~



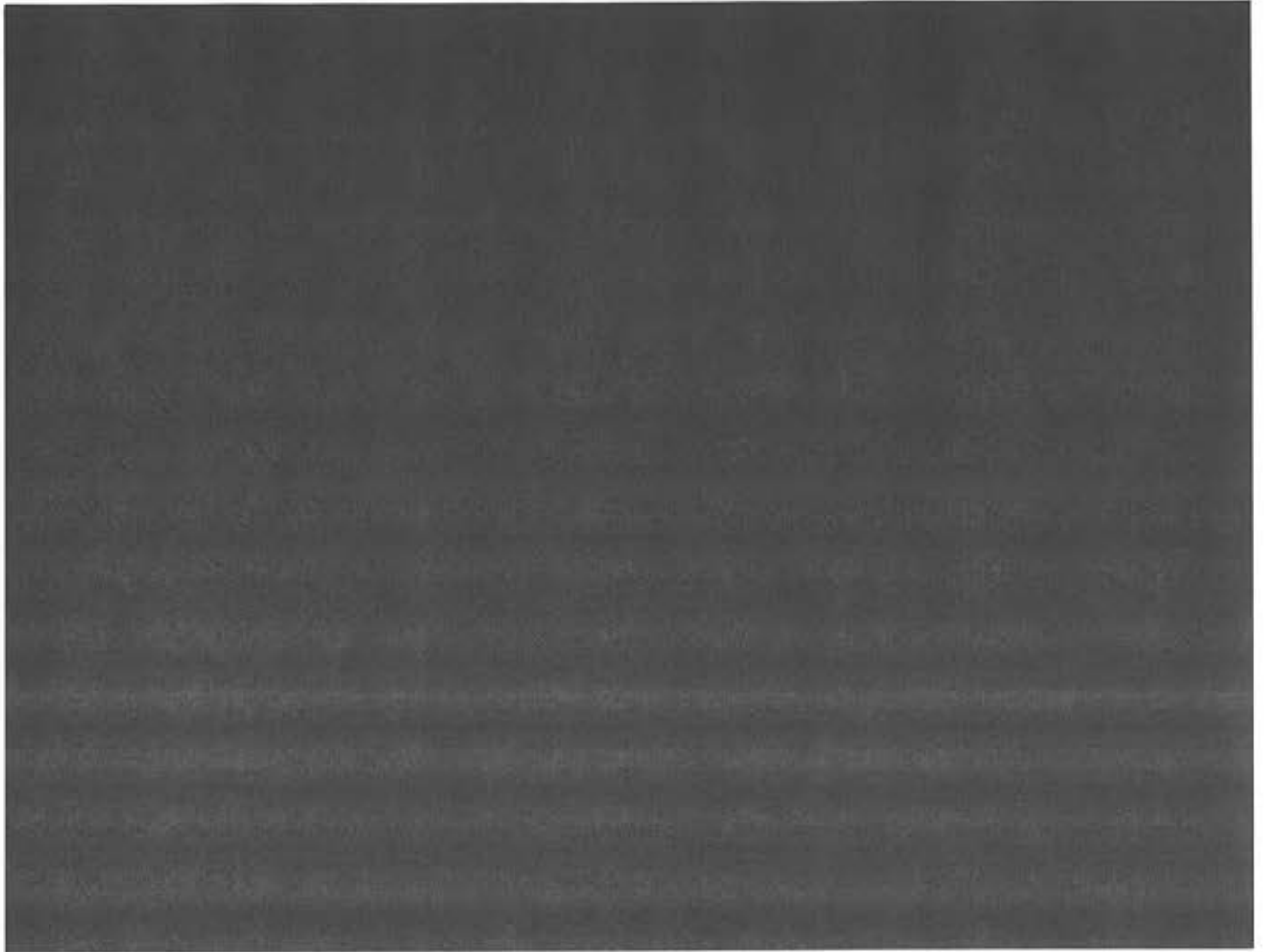
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



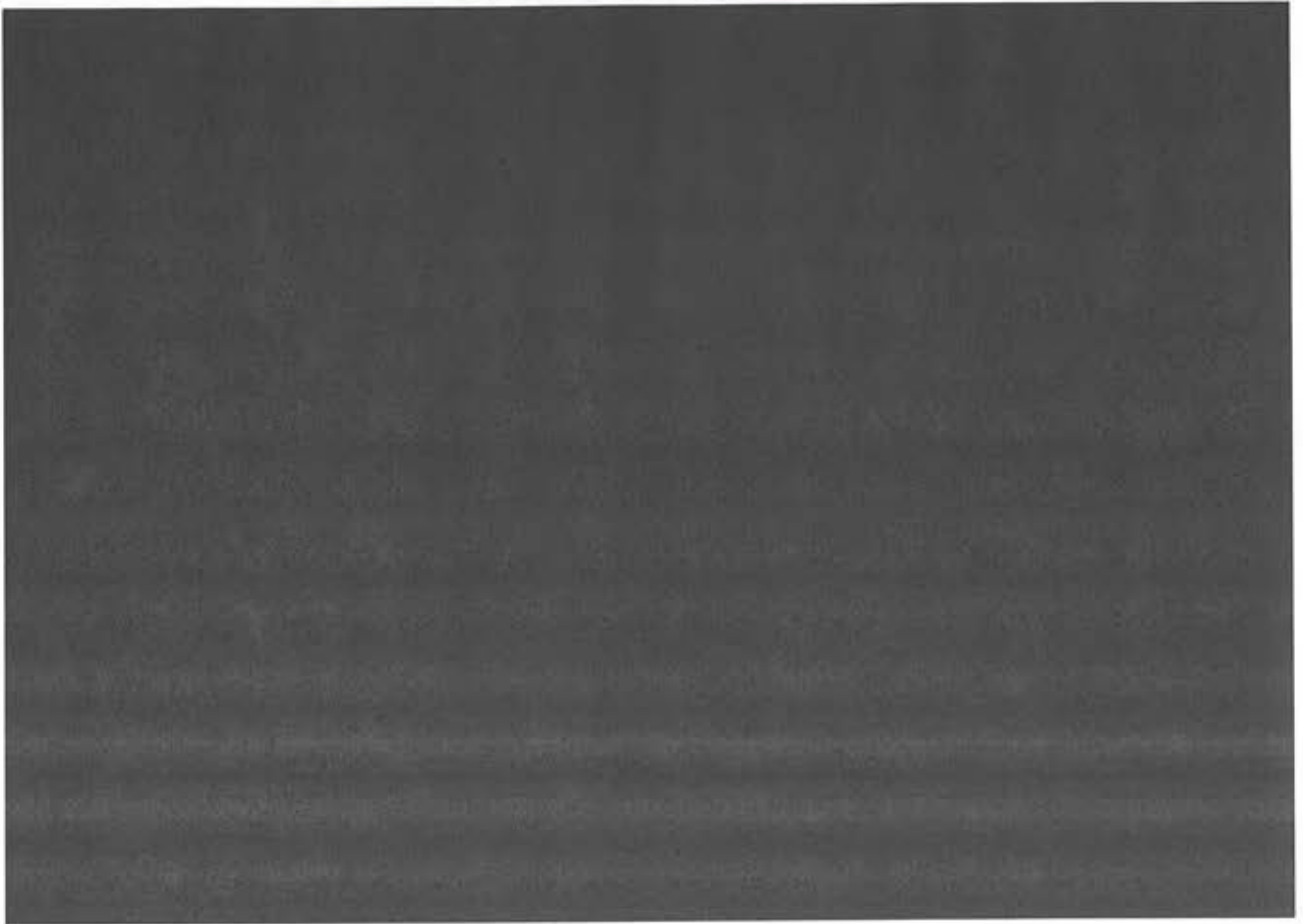
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



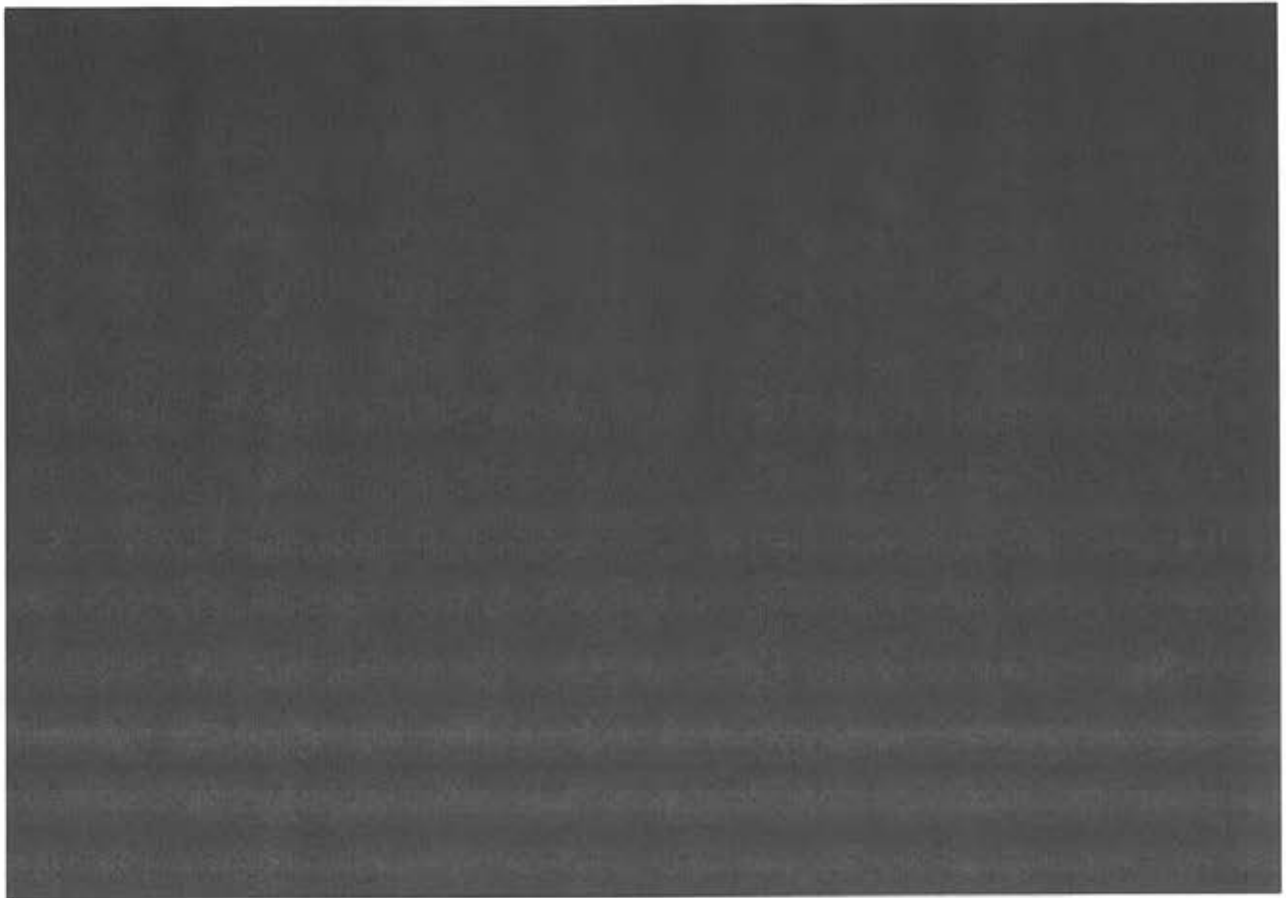
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



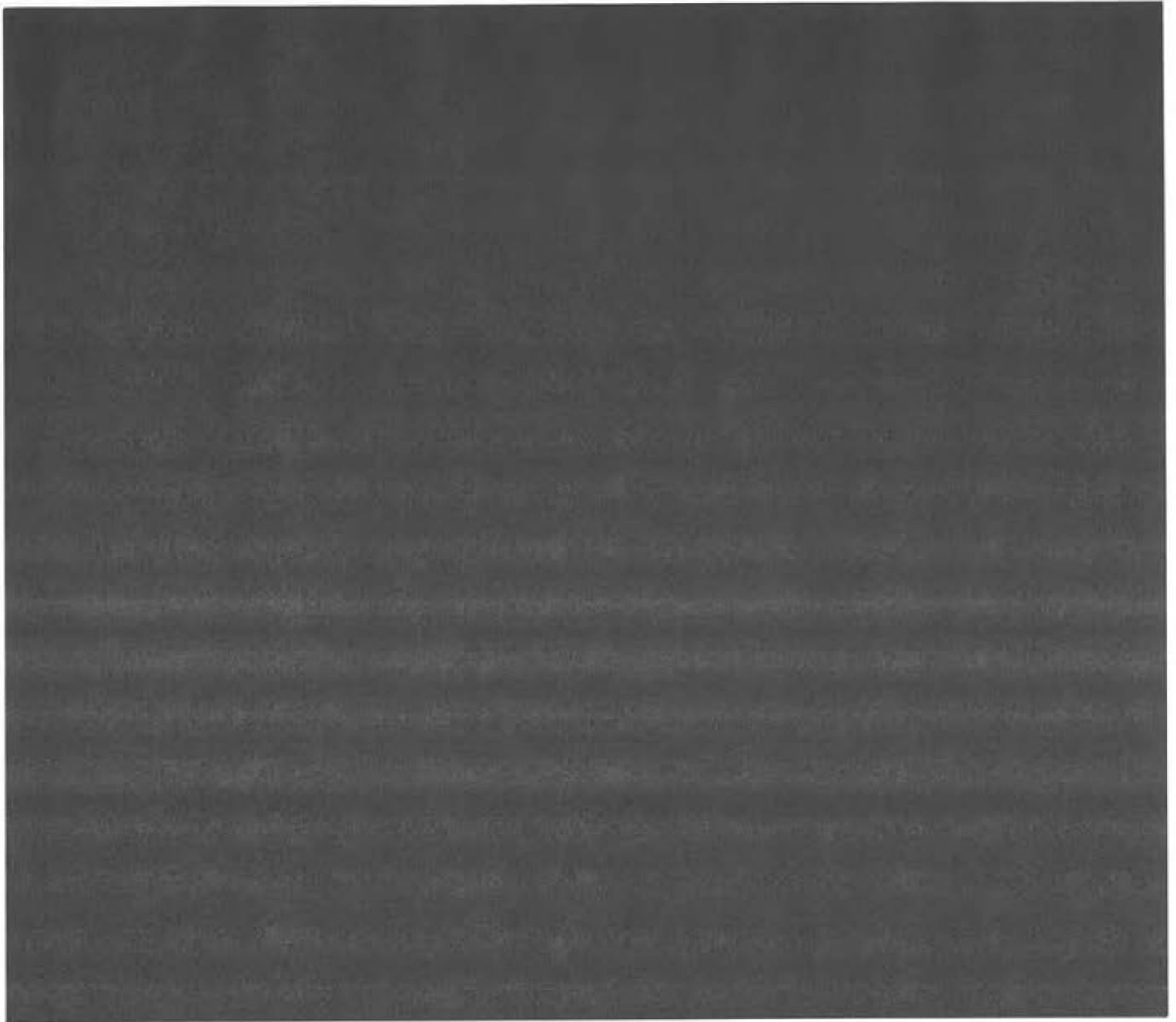
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



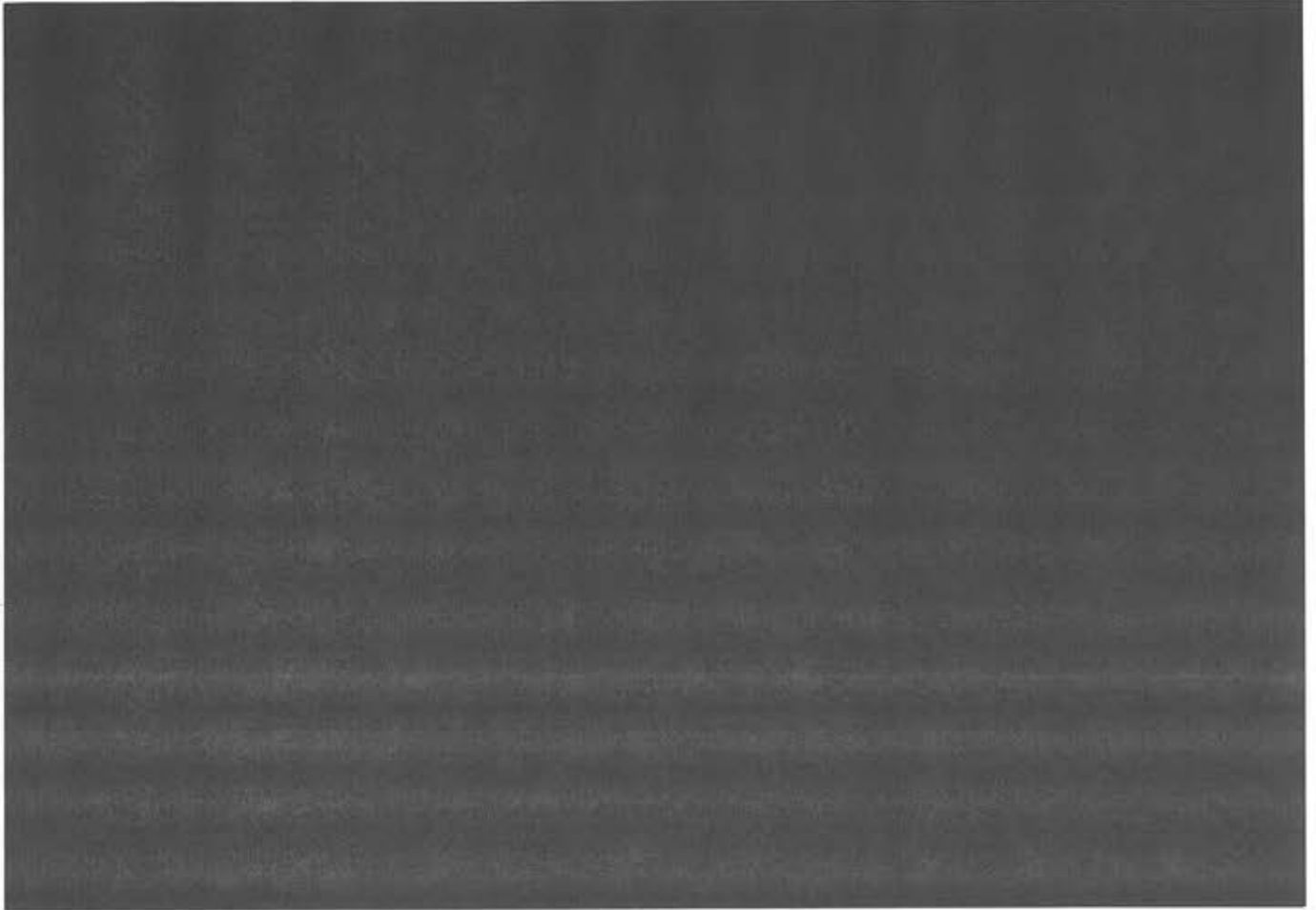
~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

~~TOP SECRET//COMINT//NOFORN//20291123~~



~~TOP SECRET//COMINT//NOFORN//20291123~~

FILED  
KAREN E. SUTTON, CLERK

MAY 14 2004

U.S. Foreign Intelligence  
Surveillance Court

~~TOP SECRET//COMINT//NOFORN//X1~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D. C.

---

IN RE ELECTRONIC SURVEILLANCE AND : Docket Number:   
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :  
AND RELATED TARGETS. ~~(S)~~ :

---

MOTION FOR CONTINUATION OF AMENDED ORDER

Introduction (U)

The United States of America, by counsel, hereby moves this Court, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 and 1821-1829 (FISA or the Act), to order the permanent continuation of its order of July 22, 2002, in the above-captioned matter. The United States seeks continuance of the order because it has been highly successful. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

Classified by: James A. Baker, Counsel for Intelligence  
Policy, OIPR, DOJ  
Reason: 1.4(c) - (d)  
Declassify on: X1

~~TOP SECRET//COMINT//NOFORN//X1~~

Because the order permits the rapid sharing of information within the United States Intelligence Community, the United States has obtained vital actionable intelligence regarding the activities, capabilities, plans and intentions of [REDACTED]

[REDACTED]

[REDACTED] The U.S. Intelligence Community process for sharing information - and taking action based upon such information - that the July 22, 2002 Order has fostered is now a vital part of the Nation's war on terrorism. The order has permitted the U.S. Intelligence Community to produce and disseminate to policy makers (including the President of the United States) a substantial volume of intelligence reports, and has enabled the United States and its allies to locate and apprehend numerous terrorists overseas and disrupt terrorist operations. As a result, we submit that the order has enhanced the ability of the United States Government to protect national security. Moreover, because of the manner in which the U.S. Intelligence Community has implemented the order, we submit that the intrusion on the privacy interests of Americans to date has been limited. (TS)

On July 22, 2002, the Court authorized the Federal Bureau of Investigation (FBI) to provide to the Central Intelligence Agency (CIA) and the National Security Agency (NSA) "raw data" (i.e.

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

unminimized information) obtained from certain searches and surveillances of terrorist targets under the FISA. The Court's Order, described below, modified the standard minimization procedures used in international terrorism cases. The Court further ordered that the "matter shall be fully considered again by the Court en banc at its annual conference in May of 2004." See July 22, 2002 Order at 5.<sup>1</sup> In this regard, on April 21, 2004, the Court directed that the Government:

[S]hall file a motion requesting continuation of that order. Such motion should include a statement that the factual circumstances relied upon by the Government in seeking approval of such procedures continue (or, to the extent they have changed, why the procedures should continue to be followed under current circumstances). ~~(S)~~

The United States, in support of this motion, states:

1. Prior to the July 22, 2002 Order, the CIA and the NSA provided linguistic and technical assistance to the FBI in analyzing unminimized foreign intelligence information, but could only use and disseminate limited, minimized data specifically disclosed to them by the FBI. On May 10, 2002, the Government filed a motion to provide raw data directly from the FBI to the

---

<sup>1</sup> The Court further ordered the Department of Justice to report every six months on the implementation of the Order. This motion incorporates information taken from the most recent report which covers the time period from September 1, 2003 to December 31, 2003. That report will be filed with the Court forthwith. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

CIA and the NSA, which those agencies would then minimize. The Government made this motion because of the need to

- (i) disseminate pertinent foreign intelligence information rapidly to the CIA and the NSA, (ii) enable these agencies to apply their analytical skills to the data directly, and
- (iii) provide maximum flexibility in applying Intelligence Community resources to international terrorist targets. In its Order, the Court granted the Government's motion with modifications. ~~(S)~~

2. The July 22, 2002 Order provided the following. The FBI may provide the CIA and the NSA raw data obtained from FBI electronic surveillances and physical searches targeting international terrorist groups and their agents, or from surveillances or searches of other targets where there is a reasonable expectation that the surveillance or search will reveal information related to international terrorism. The raw data provided may include communications of or information about U.S. persons. The CIA and the NSA may review, translate, analyze, minimize, use, retain and disseminate such information pursuant to certain minimization procedures. The NSA is to employ the standard FISA minimization procedures that it normally uses for conducting its Court-authorized surveillances, with certain modifications. Likewise, the CIA is to use procedures

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

similar to those it normally uses for the retention and dissemination of information from its non-FISA electronic surveillances, with certain modifications. ~~(S)~~

3. As described below, the FBI has successfully provided unminimized FISA information to the NSA and CIA pursuant to the Court's July 22, 2002 Order. To date, this information has consisted only of the results of Court-authorized electronic surveillance and physical searches [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Although authorized by the July 22, 2002 Order, the FBI has not provided NSA or CIA with unminimized information pursuant to the Order from other means of electronic surveillance or physical searches, such as [REDACTED]. ~~(TS)~~

4. For international terrorism cases, FBI technical personnel receive and/or retrieve the data obtained from these searches and surveillances from the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The FBI then forwards the data described above

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

from international terrorism searches and surveillances to the NSA and the CIA.<sup>2</sup> Before providing the data to the CIA, the FBI

(b)(1); (b)(3); (b)(7)(E)

NSA

The FBI retains the record copy of the communications. ~~(TS)~~

5. Pursuant to the Court's Order, the FBI electronically forwards to the NSA all international terrorism [REDACTED] that the FBI acquires from [REDACTED]

[REDACTED] The vast majority of the data that the NSA has reviewed was obtained from electronic surveillances and physical searches of non-U.S. person targets located outside the United States. From August 2002 to present, the NSA has issued over [REDACTED] intelligence reports based, at least in part, on raw FBI FISA data relating to international terrorism. The NSA has instructed its employees to include the caveat required by the July 22, 2002 Order on such

<sup>2</sup> As described below, the CIA generally receives data that it specifically requests, rather than the entire universe of terrorism-related [REDACTED] collected by FBI pursuant to FISA. ~~(TS)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

reports.<sup>3</sup> In order to ensure that its employees comply with this requirement, the NSA includes this instruction in its FISA minimization training and also has provided its employees with written reporting guidance. ~~(TS)~~

The recipient of the raw FISA data at NSA is NSA's [REDACTED] [REDACTED] in the Data Acquisition Directorate, where it is formatted and placed in a database for analysts in NSA's Office of Counterterrorism to review. Analysts at the Office of Counterterrorism are trained by attorneys from NSA's Office of General Counsel concerning the applicable minimization procedures and the Court's July 22, 2002 Order before they are permitted access to the database containing the raw FISA data. On August 20, 2002, the Attorney General signed procedures governing the NSA's dissemination of FBI FISA information identifying U.S. persons to foreign governments, a copy of which was previously provided to the Court. ~~(S//SI)~~

6. [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED] [REDACTED] The CIA also assists the  
FBI, at the FBI's request, with translations of communications of

<sup>3</sup> See May 10, 2002 Motion at [REDACTED]. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

other international terrorism targets. The CIA receives raw FISA data from the FBI [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] ~~(S//NF)~~

On August 20, 2002, the Attorney General signed procedures governing the CIA's dissemination of FISA information to foreign governments, a copy of which was previously provided to the Court. Those procedures apply to data processed and minimized by the CIA. They also apply to data minimized by the FBI and disseminated to the CIA where CIA engages in further analysis of the data. ~~(S)~~

[REDACTED]

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

[REDACTED]

[REDACTED] When conducting minimization reviews of NSA and CIA since implementation of the July 22, 2002 Order, OIPR has in particular focused on those agencies' handling of United States person information and, to date, has found that the agencies have acted in conformance with the applicable procedures. Thus, we have concluded that the implementation of the July 22, 2002 Order has had a limited effect on the privacy interests of U.S. persons. ~~(TS//SI)~~

8. Representatives from OIPR visit NSA and CIA to review those agencies' implementation of the Court's Order and adherence to minimization procedures. Both agencies appear to be handling the FISA data properly. OIPR expects to continue such visits on approximately an annual basis, and will continue to report to the Court every six months on the Government's implementation of the July 22, 2002 Order as required. OIPR also reviews the agencies' handling of raw data when it receives requests to initiate or renew FISA authority regarding [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] NSA reports that from August 2002 to present, approximately [REDACTED] percent of its requests for FISA authority (for the FBI to

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

conduct electronic surveillance and physical search of more than [REDACTED] have been based on information obtained through NSA's review of raw data. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In addition, the Department of Justice has submitted reports to Congress as required by law that have included discussions of the Court's July 22, 2002 Order. The Department, the FBI, CIA and NSA have briefed staff members of the Senate Select Committee on Intelligence and staff members of the House Permanent Select Committee on Intelligence on the Court's Order and on implementation thereof. ~~(TS)~~

[REDACTED]

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

[REDACTED]

Also in this regard, the NSA has informed OIPR that:

FBI FISA data is a critical part of NSA's mission targeting international terrorists and terrorist organizations and has yielded highly significant and very timely foreign intelligence information about [REDACTED]

[REDACTED] of international terrorist groups, [REDACTED]

It is presently the source providing the most [REDACTED]

During the last four months of 2003, FBI FISA data contributed in whole or in part to approximately [REDACTED] percent of all end product reporting from NSA's Counterterrorism Office. ~~(TS//SI//NF)~~

[REDACTED]

~~(TS//SI//NF)~~

10. The factual circumstances relied upon by the Government in seeking the initial July 22, 2002 approval to provide raw data directly to the CIA and the NSA have not changed other than those relating to the modified procedures approved by this Court in its

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

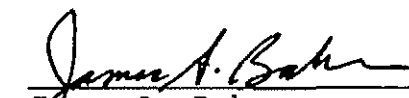
April 10, 2004 Amended Order. For this reason, the Government seeks a permanent continuation of this authority under the procedures currently in place. ~~(TS)~~

11. This motion has been reviewed for accuracy by Vito T. Potenza, Acting General Counsel, NSA; Valerie Caproni, General Counsel, FBI; and Scott W. Muller, General Counsel, CIA. (U)

WHEREFORE, the United States, by counsel, moves this Court to permit the permanent continuation of its order of July 22, 2002, in the above-captioned matter. (U)

A proposed order effecting this request accompanies this motion. (U)

Respectfully submitted,

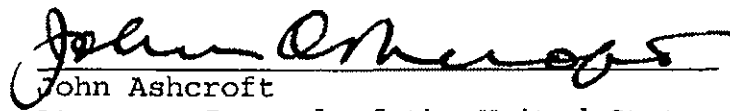
  
James A. Baker  
Counsel for Intelligence Policy  
U.S. Department of Justice

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

APPROVAL

I find that this motion satisfies the criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978, and hereby approve its filing with the United States Foreign Intelligence Surveillance Court. (U)

  
John Ashcroft  
Attorney General of the United States

OR

\_\_\_\_\_  
James B. Comey  
Deputy Attorney General of the  
United States

Dated: 5-13-04

~~TOP SECRET//COMINT//NOFORN//X1~~

FILED  
KAREN E. SUTTON, CLERK

~~TOP SECRET//COMINT//NOFORN//X1~~

MAY 19 2004

U.S. FOREIGN INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

---

IN RE ELECTRONIC SURVEILLANCE AND : Docket Number:   
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :  
AND RELATED TARGETS. ~~(S)~~ :

---

ORDER

This matter is before this Court on the May 14, 2004 motion of the United States of America seeking to continue permanently the procedures approved by the July 22, 2002 Order in the above-captioned docket. Relying upon the Motion and Order issued on July 22, 2002, as well as the facts set forth in the Government's instant motion, approved for filing by the Attorney General of the United States, the Court finds that the requested permanent

~~TOP SECRET//COMINT//SI~~

Derived from: Motion to USFISC in the above-captioned  
docket number  
Declassify on: X1

~~TOP SECRET//COMINT//NOFORN//X1~~

continuation of the procedures to the July 22, 2002 Order of this Court is warranted under the facts, and that the procedures pursuant to which the National Security Agency (NSA) and the Central Intelligence Agency (CIA) will process such material meet the definition of minimization procedures set forth in 50 U.S.C. § 1801(h) and 1821(4).

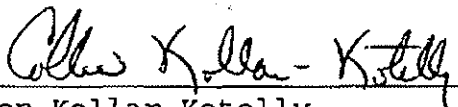
Accordingly, IT IS HEREBY ORDERED that the Federal Bureau of Investigation may continue to provide to the CIA and the NSA unminimized information obtained from searches and surveillances of terrorist targets under FISA, as set forth in the Court's July 22, 2002 Order.

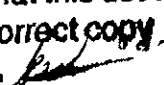
IT IS FURTHER ORDERED that all provisions of the Court's July 22, 2002 Order in docket number [REDACTED] shall remain unchanged.

Filed May 14, 2004 10:30 a.m. E.D.T.  
Date Time

Signed May 19, 2004 7:05 pm E.D.T.  
Date Time

This Order is entered with the unanimous consent of the Judges of this Court.

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

~~TOP SECRET//COMINT//NOFORN//X1~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE [REDACTED]

Docket Number:

EXHIBIT F

MEMORANDUM OF LAW IN SUPPORT OF APPLICATION FOR AUTHORITY TO  
CONDUCT ELECTRONIC SURVEILLANCE OF [REDACTED]

Derived from Application of the United States to the Foreign  
Intelligence Surveillance Court in the above-captioned  
matter  
Declassify only upon the determination of the President

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

The Government submits this memorandum of law in support of its application for authority to conduct electronic surveillance of [REDACTED]

[REDACTED] This memorandum addresses the collection of a particular type of electronic communications, i.e., "abouts" or "referred to" communications. These are communications that relate to a targeted e-mail facility used by the foreign power targets of this surveillance where the targeted e-mail address does not appear in the "to" or "from" fields of the communications.<sup>1</sup> In the Court's previous Order and Memorandum Opinion related to this surveillance, the Court instructed that, if "the government continues to seek authority for [this] type of surveillance . . . its further submissions shall include an analysis of the extent to which such surveillance is directed at selector e-mail addresses, and the extent to which it is directed at e-mail addresses that send or receive communications that are acquired because they refer to a selector e-mail address." Order and Memorandum Opinion, *In re*: [REDACTED]

[REDACTED], No. [REDACTED] (Apr. 3, 2007), at 21-22. The Government does seek authority to continue such surveillance, which was requested in the first application in No. [REDACTED] and is currently conducted under the authority granted in No. [REDACTED]. The collection of this information is critical to the continued success of the "early warning" system.<sup>2</sup>

### Types of "Abouts"

Before analyzing the collection of this type of communications under the electronic surveillance provisions of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1811, it is necessary to set forth the different categories of communications that fall within the

<sup>1</sup> Although the Government's application seeks to conduct surveillance of e-mail addresses and telephone numbers used by the foreign power targets of this surveillance, the type of authority addressed in this memorandum is relevant only to e-mail addresses.

<sup>2</sup> The National Security Agency has reviewed this memorandum of law for accuracy.

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

general category of "abouts" or "referred to" collection, i.e., the acquisition of communications where the targeted e-mail address does not appear in the "to" or "from" fields.



~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~



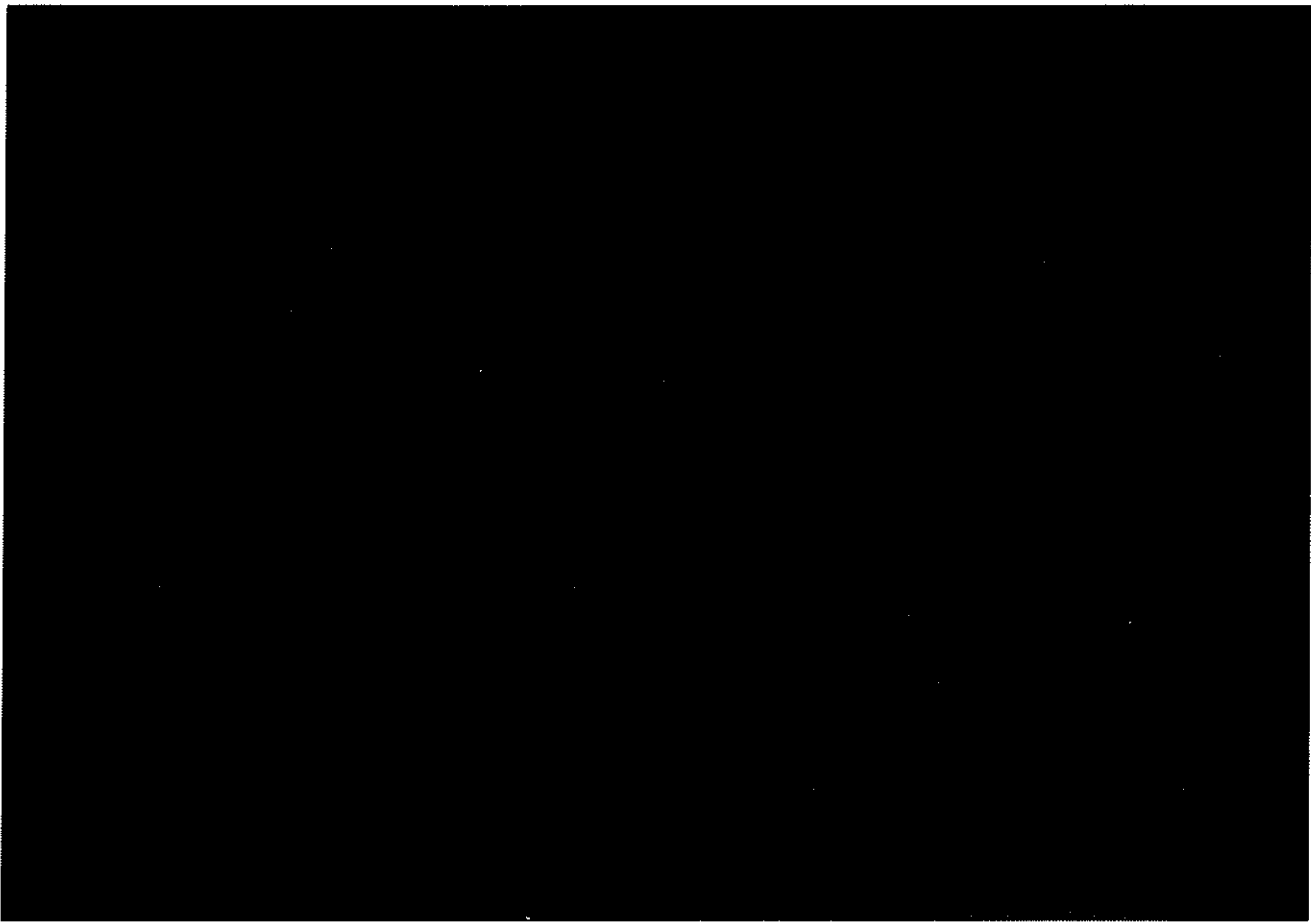
*Third-party "abouts"*

Third-party "abouts" are communications relating to a facility at which NSA is not directing surveillance that contain a targeted [REDACTED] Capturing these communications would not only provide the Government with the information contained in the text of the communication itself, but would also help to identify previously unknown terrorist associates and accounts. Third-party "abouts" include electronic communications between two

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

third-party, non-targeted facilities that contain the targeted e-mail address in the substantive contents of that communication. Thus, even when an e-mail is not to or from the targeted e-mail address, NSA would collect the communication as long as the contents of the communication contain the e-mail address. For example, [REDACTED]

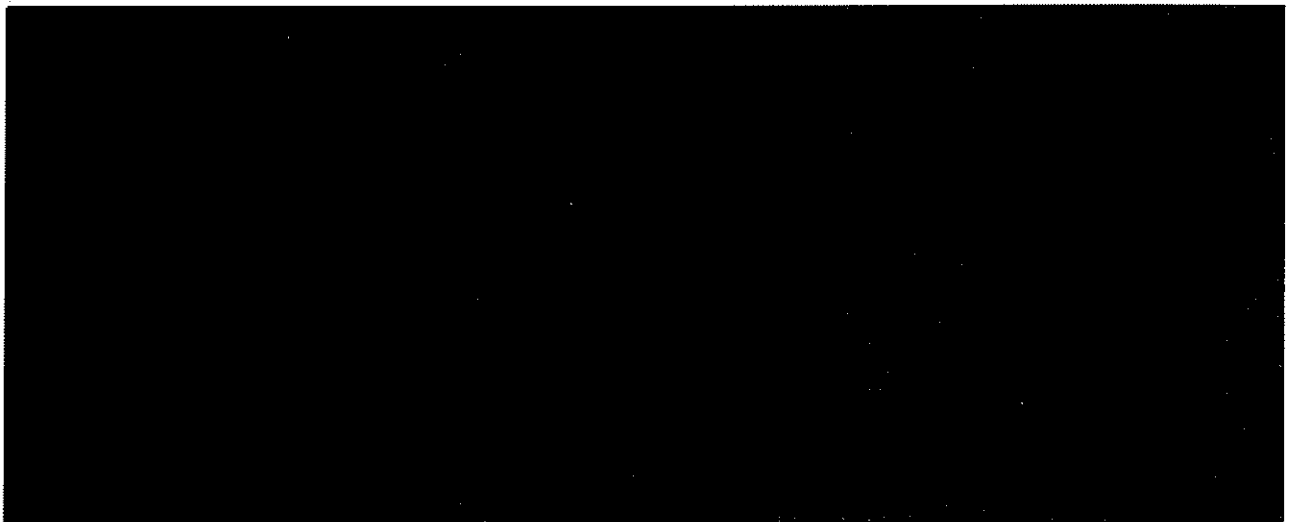
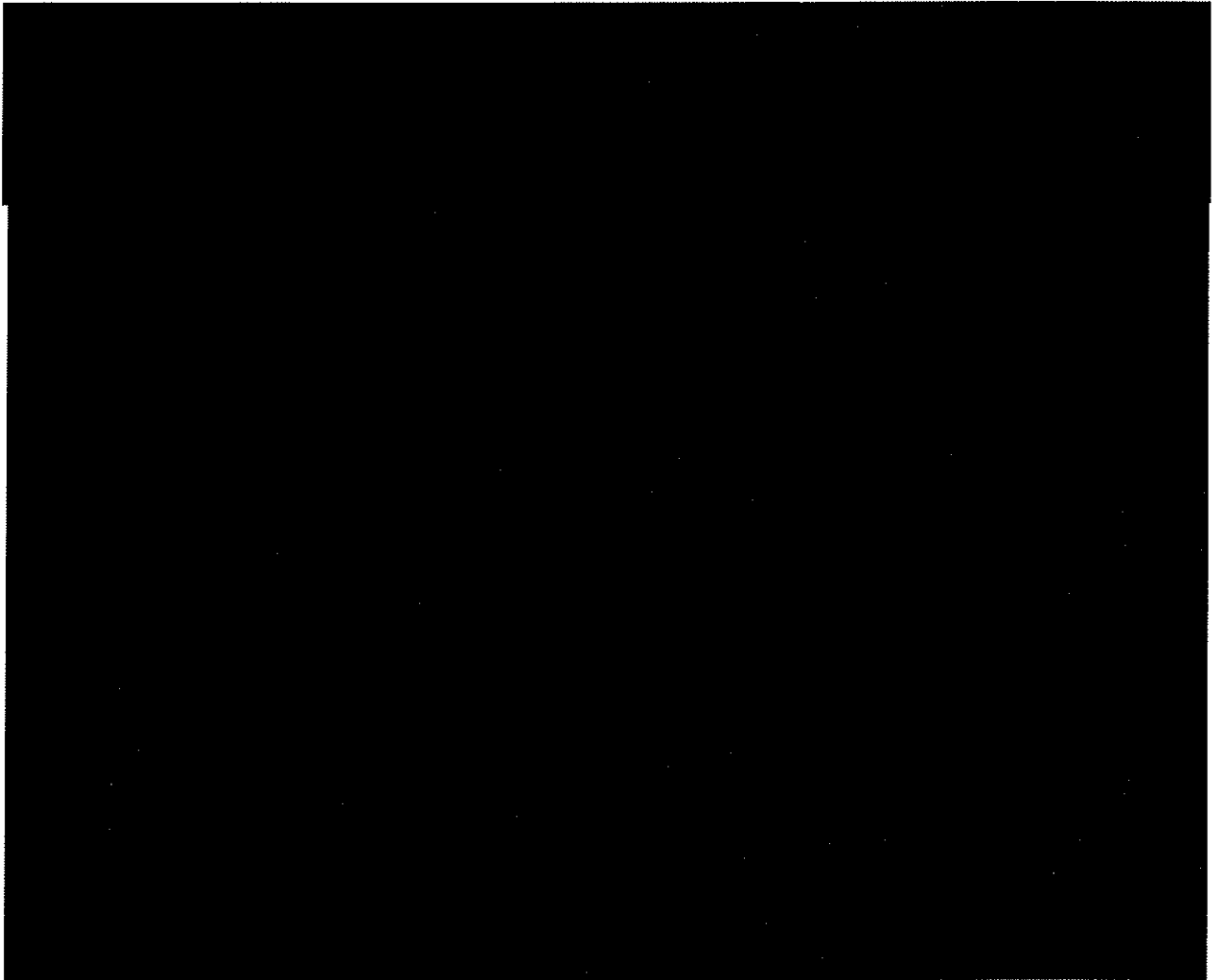


#### Legal Analysis



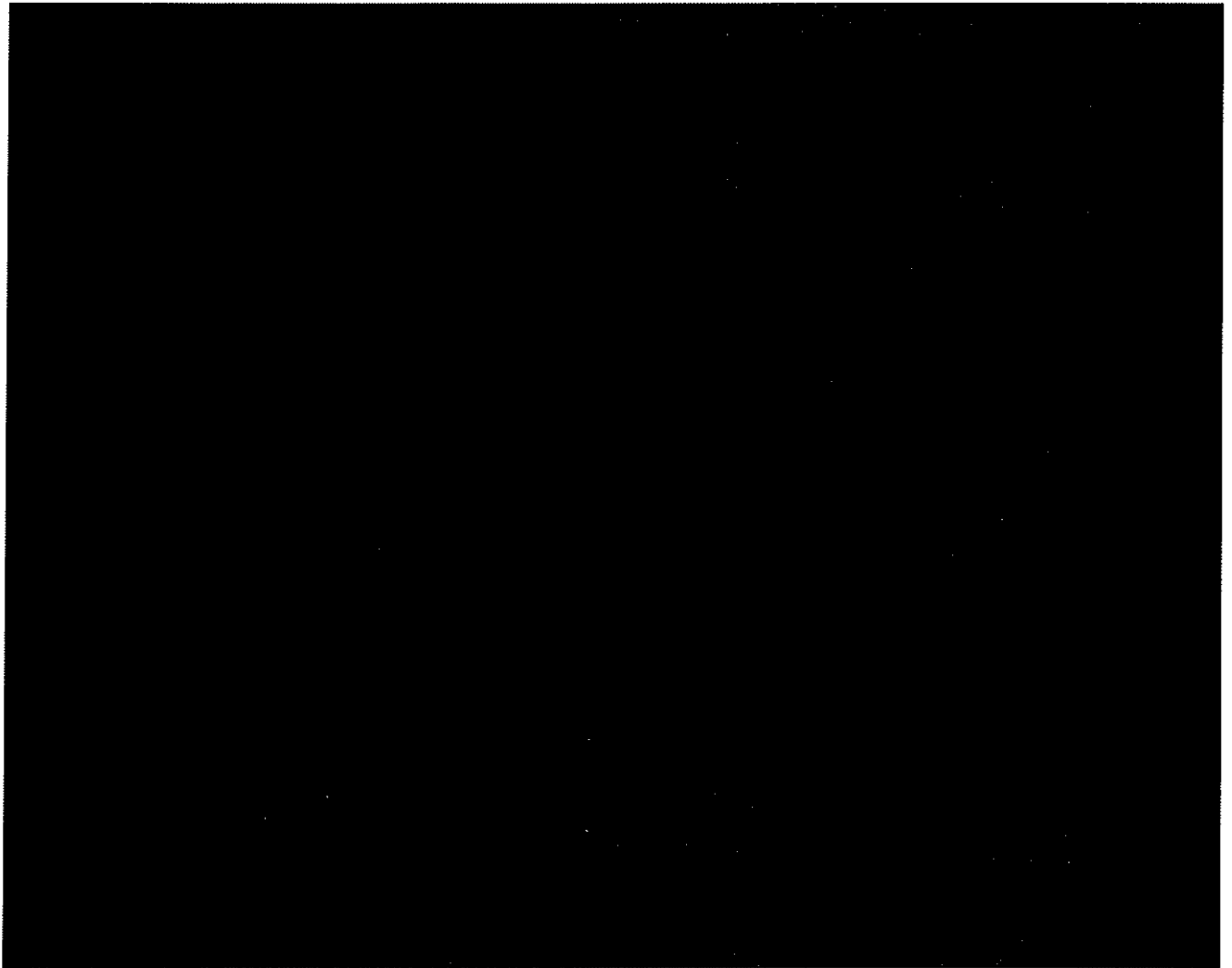
~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~



~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~



*Third-party "abouts"*

A [REDACTED] legal issue is raised by the acquisition of communications that fall within the category of third-party "abouts," i.e., where the e-mail [REDACTED] appears in the



~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

body of an e-mail neither sent nor received by an account at which surveillance is already directed [REDACTED]

[REDACTED] the communication is captured because it contains the [REDACTED] but it cannot be said that the surveillance is "directed at" the targeted account because, with respect to that particular communication, the targeted account is not "being used or about to be used" by the foreign power target. Rather, for the purposes of FISA, the surveillance is "directed at" the facilities that sent and received the communication. Nevertheless, acquisition of the communication is consistent with the statute because, at the time of acquisition, NSA has probable cause to believe that the facilities at which NSA is directing the surveillance (i.e., the previously unknown e-mail accounts) are being used by the foreign power target.

The NSA conducts this surveillance by [REDACTED]

[REDACTED]

<sup>7</sup> See Memorandum of law in support of application for authority to conduct electronic surveillance of [REDACTED]

No-

7  
~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

[REDACTED]

[REDACTED] forwarding an e-mail from that account to a third account provides probable cause to believe that either the account that is forwarding the e-mail from the targeted address or that which is receiving it is also being used by the foreign power target. And there is probable cause to believe that at least one party to a communication that mentions the e-mail address used by the target (as opposed to simply using the name of the target or of an individual associated with the target, [REDACTED]) is himself a member or agent of the target. [REDACTED]

[REDACTED] 8

It is important to note, however, the limits of such surveillance. NSA will not rely on the fact that it acquired the one communication, to begin automatically to monitor all communications of the facilities from which it acquired the communication. Rather, it will determine whether, [REDACTED]

[REDACTED] there is still probable cause to believe that the facilities are being used or are about to be used by the target of this surveillance. To be sure, regardless of whether NSA continues to collect communications of the facilities which sent and

[REDACTED]

~~TOP SECRET//SI//NF~~

~~TOP SECRET//SI//NF~~

received the acquired communication containing the targeted [REDACTED] NSA will have directed surveillance at facilities whose "nature and location . . . [are] unknown" at the time of the application. For this reason, NSA will include those facilities as part of the reporting scheme described in the application.

Accordingly, the authority the Government seeks in the application includes the authority to conduct the surveillance described above, and the acquisition of such communications is consistent with FISA.

Respectfully submitted,

Dated: May 24, 2007



Matthew G. Olsen  
Deputy Assistant Attorney General

(b)(6)  
Senior Counsel to the  
Assistant Attorney General

(b)(6)  
Attorney Advisor

National Security Division  
U.S. Department of Justice

~~TOP SECRET//SI//NF~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

2007 JUL 27 PM 3:23  
CLERK TCM

IN RE [REDACTED]

Docket Number: [REDACTED]

(U) MOTION TO AMEND

~~(TS//SI//OC,NF)~~ The United States of America, through the undersigned Department of Justice attorney, hereby moves this Court, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, Title 50, United States Code (U.S.C.), §§ 1801-1811, (FISA or the Act), for an amended order in the above-captioned docket number for the purpose of clarifying the scope of the electronic surveillance authority granted by the Court.

1. ~~(TS//SI//OC,NF)~~ Upon consideration of an application by the United States, on May 31, 2007, the Honorable Roger Vinson of this Court issued an Order in the above-captioned docket number authorizing electronic surveillance of telephone

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by: Margaret A. Skelly-Nolen, Acting Counsel for  
Intelligence Policy, NSD, DOJ

Reason: 1.4(c)

Declassify on: 27 July 2032

~~TOP SECRET//COMINT//ORCON,NOFORN~~

numbers and e-mail [REDACTED] used by [REDACTED]

[REDACTED]

[REDACTED] In the Order, the Court authorized the National Security Agency (NSA) to conduct electronic surveillance of, *inter alia*, "telephone numbers or e-mail [REDACTED] the nature and location of which are not specified [in the Order] because they were unknown to the NSA as of May 24, 2007 (the date the application was filed), where there is probable cause to believe that each additional telephone number or e-mail [REDACTED] is being used, or is about to be used" by the targeted foreign powers. Order, sub-paragraph I.b., at 11. The Court limited this authority to surveillance of additional telephone numbers and e-mail [REDACTED] that the NSA reasonably believes are being used, or are about to be used, by non-United States persons located outside the United States. *Id.*, sub-paragraph I.b., at 11-12.

2. ~~(TS//SI//OC/NF)~~ The Court further ordered that notice of any additional telephone number or e-mail [REDACTED] at which electronic surveillance is directed pursuant to the authority granted in sub-paragraph I.b. of the Order shall be provided to the Court, in accordance with 50 U.S.C. § 1805(c)(3), within twenty-one days of the date on which such surveillance begins. Order at 16. The Court ordered that the first such report shall be submitted on Wednesday, June 13, 2007, and that the report shall provide notice of additional telephone numbers and e-mail [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] for which electronic surveillance was initiated from May 24, 2007, through June 2, 2007. Id. Subsequent reports shall be submitted on a weekly basis and shall cover surveillance initiated during an earlier one-week period. Id. The Court further ordered that all such reports shall include:

- (A) the nature and location of each new facility or place at which electronic surveillance is directed;
- (B) the facts and circumstances relied upon by the United States to justify its belief that the new facility or place at which electronic surveillance is directed is or was being used, or is about to be used, by a target of surveillance;
- (C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
- (D) the total number of electronic surveillances that have been or are being conducted under the authority of this Order.

Id. at 16-17.

3. ~~(TS//SI//OC,NF)~~ To date, the Government has submitted seven reports to the Court concerning the Government use of the electronic surveillance authority granted in sub-paragraph I.b. of the Order. In response to the first report, which the Government filed on June 13, 2007, the Court (Judge Kazen) issued an order on June 22, 2007, expressing concern that "the descriptions of the targeted e-mail [REDACTED] [discussed in the June 13 report] suggest that many of the newly initiated e-mail [REDACTED] may have been known to the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

National Security Agency prior to May 24, 2007." The same concern was raised by the orders of July 6, 2007 (Judge Bates), July 6, 2007 (Judge Benson), July 13, 2007 (Judge Scullin), and July 20, 2007 (Judge Kollar-Kotelly) regarding subsequent reports filed by the Government. These orders have raised the question of what it means for a facility "at which the electronic surveillance will be directed" to be "unknown," a question that the Government did not address in the supplemented and revised application filed in the above-captioned docket number on May 24, 2007.

4. ~~(TS//SI//OC,NF)~~ Attached in support of this motion is a memorandum of law that addresses the question of what it means for the "nature and location of the facility or place at which electronic surveillance will be directed" to be "[un]known" to the NSA. For the reasons set for in the memorandum of law, the Government requests that the Court amend its May 31 Order to clarify that the NSA may initiate electronic surveillance of a facility in accordance with the May 31 Order if the NSA, or the FBI at the request or recommendation of the NSA, had not as of May 24, 2007: applied to this Court for authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1804(a) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; obtained authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1805(f) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; or tasked that facility for collection under the Terrorist Surveillance Program as of December 31, 2006, or under the authority granted

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

by this Court in docket number [REDACTED] All other provisions of this Court's original orders, dated May 31, 2007, will remain unaffected, including the date and time of expiration of the electronic surveillance. ~~(TS//SI//OC,NF)~~

~~(TS//SI//OC,NF)~~ WHEREFORE, the United States of America, through the undersigned attorney, moves this Court to issue an amended Order. A proposed order effecting this request regarding [REDACTED]

[REDACTED] is attached.

Respectfully submitted,



Matthew G. Olsen  
Deputy Assistant Attorney General

(b)(6)

Acting Deputy Assistant Attorney General

(b)(6)

Attorney-Advisor

National Security Division  
U.S. Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

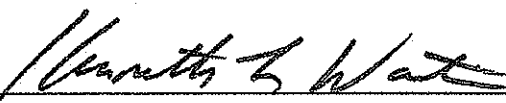
~~TOP SECRET//COMINT//ORCON,NOFORN~~

(U) APPROVAL

~~(S)~~ I find that this motion regarding [REDACTED]

[REDACTED]

satisfies the criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978, as amended, and hereby approve its filing with the United States Foreign Intelligence Surveillance Court.

  
Kenneth L. Wainstein  
Assistant Attorney General for National Security

7/27/07  
Date

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE [REDACTED]

[REDACTED] : Docket Number: [REDACTED]  
[REDACTED] :  
[REDACTED] :

MEMORANDUM OF LAW IN SUPPORT OF MOTION TO AMEND

The Government submits this memorandum in support of its motion to amend the Order of May 31, 2007, in *In re* [REDACTED]

[REDACTED] No. [REDACTED] This memorandum addresses an issue raised by subsequent orders of the Foreign Intelligence Surveillance Court ("Court") concerning electronic surveillance of telephone numbers and e-mail [REDACTED] initiated after the Government's second application.<sup>1</sup> Specifically, these orders have raised the question of what it means for a facility "at which the electronic surveillance will be directed" to be "unknown," a question that the Government did not address in its application. As set forth more fully

<sup>1</sup> See Orders of June 22, 2007 (Judge Kazen), July 6, 2007 (Judge Bates), July 6, 2007 (Judge Benson), July 13, 2007 (Judge Scullin), and July 20, 2007 (Judge Kollar-Kotelly). In light of the clarification requested by this motion and the requirements of the FISA as explained in this memorandum, the Government requests relief from that part of the Order of June 22, 2007, that directs the Government to "confirm when NSA first knew of the existence of each of [REDACTED]" discussed in the report filed on June 13, 2007. Order of June 22, 2007, at 2. The Government will, however, provide the Court with a statement confirming that as of May 24, 2007, NSA did not know that it would direct electronic surveillance at those [REDACTED] facilities.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by: Margaret A. Skelly-Nolen, Acting Counsel for Intelligence Policy, NSD, DOJ

Reason: 1.4(c)

Declassify on: 27 July 2032

~~TOP SECRET//COMINT//ORCON,NOFORN~~

below, the Government requests that the Court amend its May 31 Order to clarify that the NSA may initiate electronic surveillance of a facility in accordance with the May 31 Order if the NSA, or the FBI at the request or recommendation of the NSA, had not as of May 24, 2007: applied to this Court for authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1804(a) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; obtained authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1805(f) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; or tasked that facility for collection under the Terrorist Surveillance Program as of December 31, 2006, or under the authority granted by this Court in docket number [REDACTED] ~~(TS//SI//OC,NF)~~

The electronic surveillance that the Court approved in No. [REDACTED] allowed the Government to continue surveillance vital to the nation's security under the terms of FISA, as interpreted in the Court's Order and Memorandum Opinion of April 3, 2007. In part, the May 31 Order allowed the Government to initiate surveillance of new e-mail addresses and telephone numbers during the period of authorized surveillance and to report this initiation to the Court. This authority was critical to allowing the Government to continue the surveillance with the speed and agility necessary for its effective operation. Specifically, the Order authorized the Government, when it had the requisite probable cause, "to conduct electronic surveillance of any other telephone numbers or e-mail [REDACTED] the nature and location of which are not specified herein because they were unknown to the NSA as of May 24, 2007 (the date the application was filed) . . . ." The Court limited this authority to those facilities reasonably believed to be used by non-United States persons outside the United States. The authority was predicated on section 1805(c)(1)(B), which states that the order authorizing electronic surveillance shall specify "the nature and location of the facilities or places at which the electronic surveillance will be directed, *if known*." *Id.* (emphasis added). This language is mirrored in the section 1805(c)(3)(B) reporting requirement, which applies "where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown. . . ." *Id.* ~~(TS//SI//OC,NF)~~

Pursuant to this reporting requirement and the Court's May 31 Order, the Government submitted its first report on June 13, 2007. The Court (Judge Kazen) then

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

issued an order on June 22 expressing concern that "the descriptions of the targeted e-mail [REDACTED] suggest that many of the newly initiated e-mail [REDACTED] may have been known to the National Security Agency prior to May 24, 2007." The same question was raised by the orders of July 6, 2007 (Judge Bates), July 6, 2007 (Judge Benson), July 13, 2007 (Judge Scullin), and July 20, 2007 (Judge Kollar-Kotelly). The Government submits this memorandum to address the question of what it means for the "nature and location of the facility or place at which electronic surveillance will be directed" to be "[un]known." ~~(TS//SI//OC,NF)~~

The terms of FISA indicate that what NSA must not know at the time of the application is that it will direct electronic surveillance authorized by the order at the particular facility or place that it later adds to the surveillance. The terms "if known" in section 1805(c)(1)(B) and "unknown" in section 1805(c)(3)(B) refer to the immediately preceding phrase, "the nature and location of the facility or place at which the electronic surveillance will be directed." The words "at which the electronic surveillance will be directed" qualify the meaning of "nature and location of the facility or place." Thus, what must be not "known" or "unknown" to NSA is that it will direct "the electronic surveillance" at the facilities. The phrase "the electronic surveillance," in turn, refers back to electronic surveillance approved under FISA in that particular order. *Id.* § 1805(c)(1) ("An order approving an electronic surveillance under this section shall specify . . . the nature and location of each of the facilities at which the electronic surveillance will be directed, if known . . ."). Under the terms of FISA, then, NSA may direct surveillance at a new facility provided that it did not know, at the time of the application, that it would do so as part of the surveillance authorized by the order.

~~(TS//SI//OC,NF)~~

There are a variety of reasons why the NSA might not know at the time of the application that it would not direct electronic surveillance at a particular facility. First, the NSA might never have come across the telephone number or e-mail address. For example, [REDACTED]

[REDACTED] Second, the NSA might have had the e-mail address stored in a database but have lacked reason or the probable cause required to initiate surveillance. Third, the NSA may have had reason to initiate surveillance under another of its

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

programs outside FISA, but did not know at the time of the application that the telephone number was linked to the foreign power targets of this authorized collection. In this case, for instance, later analysis and collection could have revealed that the number was used by [REDACTED]. There may be other circumstances as well in which NSA will not have known at the time of the application that it will direct surveillance at a facility it later wants to include. In some of these cases, the phone number or e-mail

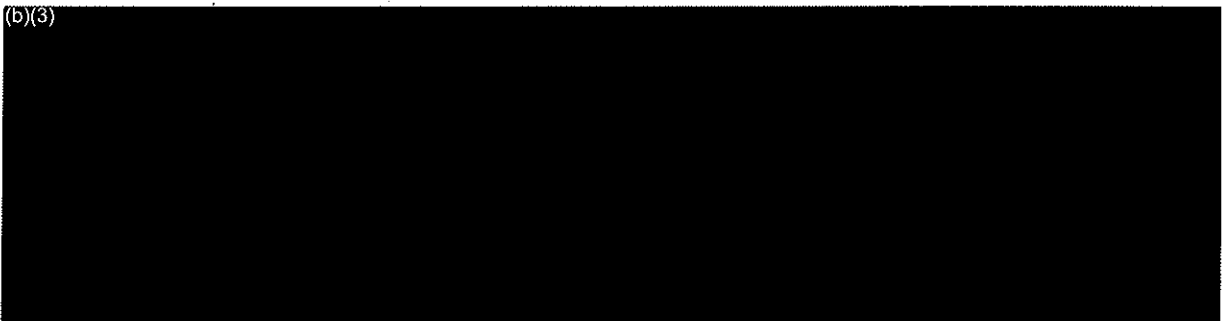
[REDACTED] will be known to NSA generally and in others the phone number or e-mail [REDACTED] will not be known to NSA. But in all of these cases, NSA did not know at the time of the application that it would direct electronic surveillance at this facility. Moreover, in many instances, when an NSA analyst decides to initiate surveillance of a facility under this Order, the analyst will simply not know whether the facility was the subject of previous collection in another of NSA's programs.<sup>2</sup> ~~(TS//SI//OC,NF)~~

Other interpretations of section 1805(c)(1)(B) and 1805(c)(3) would not only be inconsistent with their plain terms, but would be unworkable for NSA. Requiring that no part of NSA had ever known of the existence of the e-mail address or telephone number would ignore that the complete phrase that immediately precedes "unknown" and "if known" is "the nature and location of the facility or place at which the electronic surveillance will be directed," not just "the nature and location of the facility or place."

~~(TS//SI//OC,NF)~~

In other types of surveillance where the Government uses the authority that triggers the section 1805(c)(3) reporting requirement, this reading of FISA would have absurd results. For instance, the Court authorizes the Government to conduct mobile audio surveillance although the "nature and location of each of the facilities or places at

(b)(3)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

which the electronic surveillance will be directed" is unknown at the time of the application. The Government may then use this authority to conduct surveillance of the target in a park. It then reports to the Court that it directed the surveillance at that park. Of course, the Government knew of the park at the time of the application. But what it did not know is that it would be directing surveillance authorized by the order at that park. In the same way, the NSA may know of an e-mail [REDACTED] or telephone number, but not know, at the time of the application, that it would be directing surveillance at that facility under the Court's order. ~~(TS//SI//OC,NF)~~

Such a requirement would also mean that NSA would have to check multiple databases concerning all of its other programs to ensure that it had not come across the e-mail address or telephone number previously. If it had, NSA could not utilize the authority. More seriously, NSA is not able to undertake this burdensome task of verification. Because NSA can not ensure that it never previously knew of the facility through any of its surveillance programs, the implication of any such requirement would be that NSA could not utilize the authority envisioned by FISA and granted by the Court—an authority necessary to conduct the surveillance with the speed and agility needed to protect the nation's security. ~~(TS//SI//OC,NF)~~

Although FISA requires only that NSA not have known that it would direct surveillance at a facility as part of the authorized surveillance, the Government requests a more limited use of this authority. In order to ensure that NSA complies with this statutory requirement in a manner that is easy to administer, the Government requests that the Court amend its order to make clear that the NSA may use the authority to initiate electronic surveillance of a facility if the NSA, or the FBI at the request or recommendation of the NSA, had not as of May 24, 2007: applied to this Court for authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1804(a) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; obtained authority to conduct electronic surveillance of that facility under 50 U.S.C. § 1805(f) as a facility used by one of the foreign power targets of this surveillance or by one of their agents; or tasked that facility for collection under the Terrorist Surveillance Program as of December 31, 2006, or under the authority granted by this

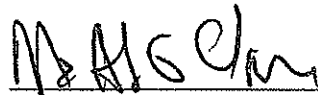
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Court in docket number [REDACTED].<sup>3</sup> This authority would be consistent with but more limited than that allowed by FISA, because NSA could not use the authority even if it did not know at the time of the application that it would want to direct the surveillance authorized by the Court in [REDACTED] at the facility. But the limitation the Government proposes makes the determination an objective one that is easier for the Government to administer and the Court to verify. ~~(TS//SI//OC,NF)~~

For the reasons set forth above, the Government respectfully requests that the Court grant its motion for clarification and to amend. (U)

Respectfully submitted,



Matthew G. Olsen

Deputy Assistant Attorney General

(b)(6)

Acting Deputy Assistant Attorney General

(b)(6)

Attorney-Advisor

National Security Division  
U.S. Department of Justice

<sup>3</sup> Several of the facilities at which NSA directed surveillance using the authority discussed in this memorandum were facilities that had previously been tasked under FISA. See 13 June Report Pursuant to 50 U.S.C. § 1805(c)(3), Attachment B Bates Numbers [REDACTED]. For the reasons explained above, this surveillance was consistent with FISA. Nevertheless, their continued tasking would be inconsistent with the clarification the Government now proposes. Therefore, the Government will discontinue conducting surveillance of these facilities using this authority. ~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~