Office of the Director of National Intelligence
Washington, DC 20511

DEC 15 2014

Mr. Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Reference: DF-2014-00200

Dear Mr. Crocker:

This letter responds to your letter dated 6 May 2014 (Enclosure 1), pursuant to the Freedom of Information Act (FOIA), seeking ***"all records, emails and communications related to the development or implementation of the 'Vulnerabilities Equity Process' and all records, emails and communications related to or reflecting the 'principles' that guide the agency 'decision-making process for vulnerability disclosure in the process described in the White House blog post.'".***

The ODNI has located documents responsive to that request, as subsequently modified by the court's order of 21 October 2014. Enclosed are three documents that are being released in segregable form with deletions made pursuant to FOIA exemptions (b)(1), (b)(3), (b)(5) and (b)(6) (Enclosure 2). In addition, three other responsive documents have been denied in their entirety pursuant to FOIA exemptions (b)(1), (b)(3), and (b)(5).

Exemption (b)(1) protects classified information under Executive Order 13526, Section 1.4(c). Exemption (b)(3) applies to information exempt from disclosure by statute. The relevant withholding statute is the National Security Act of 1947, as amended, 50 U.S.C. § 3024(i)(1), which protects information pertaining to intelligence sources and methods. Exemption (b)(5) protects privileged interagency or Intra-Agency information. Exemption (b)(6) applies to records which, if released, would constitute a clearly unwarranted invasion of the personal privacy of individuals.

At this time, your FOIA request remains open, and the ODNI will continue to process your request and provide a further response on or about 15 January 2015.

Sincerely,

Jennifer Hudson
Director, Information Management Division

Enclosures

ENCLOSURE

1

DF.2014.00200

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

May 6, 2014

Pamela N. Phillips
National Security Agency
Chief, FOIA/PA Office (DJP4)
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

MAY 07 2014

BY FACSIMILE: (443) 479-3612

Jennifer L. Hudson
Director, Information Management Division
Office of the Director of National Intelligence
Washington, D.C. 20511

BY FACSIMILE: (703) 874-8910

RE: Freedom of Information Act Request
Request for Expedited Processing

Dear Ms. Phillips and Ms. Hudson:

This letter constitutes an expedited request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the National Security Agency ("NSA") and the Office of the Director of National Intelligence ("ODNI") on behalf of the Electronic Frontier Foundation ("EFF"). EFF makes this request as part of its Transparency Project, which works to obtain government records and make those records widely available to the public.

On April 12, 2014, Bloomberg News published a story alleging that the NSA had knowledge of the Internet security flaw known as Heartbleed, and that the Agency had secretly exploited the vulnerability for intelligence gathering purposes for at least two years.[1] The ODNI quickly refuted this story. It explained that in response to recommendations by the White House Review Group, the executive branch had "reviewed its policies in this area and reinvigorated an interagency process for deciding when to share vulnerabilities. This process is called the Vulnerabilities Equities Process."[2] A subsequent blog post by the White House Cybersecurity Coordinator explained that the government, including the NSA, had "established principles to

[1] Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*, Bloomberg (Apr. 11, 2014), http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

[2] ODNI, *Statement on Bloomberg News story that NSA knew about the "Heartbleed bug" flaw and regularly used it to gather critical intelligence* (Apr. 11, 2014), http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew.

815 Eddy Street - San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

guide agency decision-making . . . a disciplined, rigorous and high-level decision-making process for vulnerability disclosure."[3] Accordingly, EFF hereby requests the following records:

All records, emails and communications related to the development or implementation of the "Vulnerabilities Equity Process" and all records, emails and communications related to or reflecting the "principles" that guide the agency "decision-making process for vulnerability disclosure" in the process described in the White House blog post.

Request for Expedited Processing

For the reasons discussed below, a "compelling need" exists for the records sought in this request, and, as such, EFF is entitled to expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II) and 32 C.F.R. § 299.5(f)(2) (NSA FOIA regulations) and 32 C.F.R. § 1700.12 (ODNI FOIA regulations).

Expedited Processing under 32 C.F.R. § 299.5(f)(2) and 32 C.F.R. § 1700.12

EFF is entitled to expedited processing because the request pertains to information about which there is an "urgency to inform the public about an actual or alleged federal government activity," and the request is "made by a person primarily engaged in disseminating information." 32 C.F.R § 1700.12(c)(2) *see also* 32 C.F.R. § 299.5(f)(2). The information we request easily satisfies this standard.

First, the records sought by this request undeniably concern a "federal government activity." *Id.* The records requested here concern the activity of several agencies of the Executive Branch and reflect on the federal government's decision-making processes.

Second, there is an "urgency to inform the public" about the federal government activity. *Id.* As the conflict between the Bloomberg News story and the responses by the government indicate, there is an ongoing debate about whether and under what circumstances the government should choose not to disclose computer vulnerabilities it is aware of. In particular, the Review Group on Intelligence and Communications Technologies appointed by President Obama to assess the NSA's activities released a report in December 2013 addressing this issue,[4] and debate continues within the government and in the press.[5]

---

[3] Michael Daniel, Cybersecurity Coordinator, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House (Apr. 28, 2014), http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[4] *See* President's Review Grp. on Intelligence and Commc'ns Tech., *Liberty and Security in a Changing World* 37 (Dec. 12, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[5] *See, e.g.*, David E. Sanger, *White House Details Thinking on Cybersecurity Flaws*, N.Y. Times (Apr. 28, 2014), http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html; Jack Goldsmith, *Thoughts on White House Statement on Cyber*

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

In two recent FOIA cases brought by EFF, the court found that requests warranted expedited treatment where Congress is considering legislation "and the records may enable the public to participate meaningfully in the debate over such pending legislation." *EFF v. ODNI*, 542 F. Supp. 2d 1181, 1187 (N.D. Cal. 2008) (citing *EFF v. ODNI*, 2007 U.S. Dist. LEXIS 89585 (Nov. 27, 2007)). Even though the court could not "predict the timing of passage of the legislation" the court granted expedited processing, holding "that delayed disclosure of the requested materials may cause irreparable harm to a vested constitutional interest in 'the uninhibited, robust, and wide-open debate about matters of public importance that secures an informed citizenry.'" *Id.* (citing *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)). Similarly, there is an urgency to inform the public about the information we seek here.

Further, as explained below in support of our request for "news media" treatment, EFF is "primarily engaged in disseminating information" under 32 C.F.R. §299.5(f)(2) and 32 C.F.R § 1700.12(c)(2).

Therefore, this request meets the standard for expedited processing set forth in 32 C.F.R. § 299.5(f)(2) and 32 C.F.R. §.1700.12.

Request for News Media Fee Status

EFF asks that it not be charged search or review fees for this request because EFF qualifies as a representative of the news media pursuant to the FOIA and 32 C.F.R. § 286.28(e)(7) and 32 C.F.R. § 1700.2(h)(4). In requesting this classification, we note that the Department of Homeland Security ("DHS") and NSA, among other agencies, have recognized that EFF qualifies as a "news media" requester, based upon the publication activities set forth below (see DHS stipulation and NSA letter, attached hereto). We further note that the U.S. Court of Appeals for the D.C. Circuit has stressed that "different agencies [must not] adopt inconsistent interpretations of the FOIA." *Al-Fayed v. CIA*, 254 F.3d 300, 307 (D.C. Cir. 2001), quoting *Pub. Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1287 (D.C. Cir. 1983).

EFF is a non-profit public interest organization that works "to protect and enhance our core civil liberties in the digital age."[6] One of EFF's primary objectives is "to educate the press, policymakers and the general public about online civil liberties."[7] To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

Vulnerabilities, Lawfare (Apr. 28, 2014), http://www.lawfareblog.com/2014/04/thoughts-on-white-house-statement-on-cyber-vulnerabilities (noting conflict between White House report and policy announced in blog post); Julian Sanchez, *The NSA's Heartbleed problem is the problem with the NSA*, Guardian (Apr. 12, 2014), http://www.theguardian.com/commentisfree/2014/apr/12/the-nsas-heartbleed-problem-is-the-problem-with-the-nsa.

[6] Guidestar Nonprofit Report, Electronic Frontier Foundation, https://www.guidestar.org/organizations/04-3091431/electronic-frontier-foundation.aspx (last visited August 22, 2013).

[7] *Id.*

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

First, EFF maintains a frequently visited web site, http://www.eff.org, which received 1,314,234 unique visitors in July 2013 — an average of 1,776 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.

EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 235,000 subscribers. A complete archive of past EFFectors is available at http://www.eff.org/effector/.

Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (http://www.eff.org/deeplinks/) reports and analyzes newsworthy developments in technology. DeepLinks had 116,494 unique visitors in July 2013. EFF also maintains a presence on the social media networks Twitter (more than 140,000 followers), Facebook (more than 67,000 followers), and Google Plus (more than 2,000,000 followers).

In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than forty white papers published since 2003. These papers, available at http://www.eff.org/wp/, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.

EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (http://www.powells.com). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (http://www.amazon.com). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at http://cryptome.org/cracking-des.htm and for sale at Amazon.com.

Request for a Public Interest Fee Waiver

EFF is entitled to a waiver of duplication fees because disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(a)(iii) and 32 C.F.R. § 286.28(d)(1) and 32 C.F.R. § 1700.6(b)(2). To determine whether a request meets this standard, the agency determines whether "[d]isclosure of the requested information . . . is likely to contribute significantly to public understanding of the operations or activities of" the government, 32 C.F.R. § 286.28(d)(1); 32 C.F.R. § 1700.6(b)(2)., and whether such disclosure "is not primarily in the commercial interest of the requester." *Id.* This request satisfies these criteria.

First, the records requested are created by federal agencies and therefore necessarily implicate "the operations or activities of" the government." 32 C.F.R. § 286.28(d)(1); 32 C.F.R. § 1700.6(b)(2).

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

Second, disclosure of the requested information will contribute to a public understanding of government operations or activities. *Id.*. EFF has requested information that will shed light on the government's decision-making process with regard to computer vulnerabilities. EFF will make the information it obtains under the FOIA available to the public and the media through its web site and newsletter, which highlight developments concerning privacy and civil liberties issues, and/or other channels discussed more fully above.

Finally, since only limited information has been made available regarding this decision-making process, the disclosure will "contribute significantly" to the public's knowledge and understanding of these activities. *Id.* Disclosure of the requested information will help inform the public about the criteria used by the government in deciding whether to disclose vulnerabilities and the wisdom of these activities.

Furthermore, a fee waiver is appropriate here because EFF has no commercial interest in the disclosure of the requested records. 32 C.F.R. § 286.28(d)(1); 32 C.F.R. § 1700.6(b)(2). EFF is a 501(c)(3) nonprofit organization and will derive no commercial benefit from the information at issue here.

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact me at (415) 436-9333 x139 or andrew@eff.org. As FOIA provides, I will anticipate a determination on this request for expedited processing within 10 calendar days.

I certify that, to the best of my knowledge and belief, all information within this request is true and correct.

Sincerely,

/s/ Andrew Crocker

Andrew Crocker, Esq.
Legal Fellow

Enclosure

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

ENCLOSURE

2

Doc 009
Release in Part
(b)(1)(b)(6)

~~SECRET//20330207~~

NSPD-54/HSPD-23 Paragraph (49) Plan Working Group

CNCI *Connect the Centers* Team Meeting

Meeting Agenda

28 July 2008, 1500-1600
CIA OHB Room 6G33

Topics for Disucssion

Para (49) Plan Discussion (Outline of Plan):

- [redacted] (b)(1)
- [redacted]
  1. Sharing of known vulnerabilities. [redacted] (b)(1)
- Recommendations: [redacted] (b)(1), (b)(5)
  8. Vulnerabilities Equities [redacted]

[redacted] Non-responsive

CL BY: [redacted] (b)(6)
CL REASON: 1.4(c), (g)
DECL ON: 20330207
DRV FROM: MIS S-06

~~SECRET//20330207~~

Non-responsive

~~SECRET//20330207~~

[redacted]

[redacted]

Questions to be discussed:

[redacted] (b)(3)

a. Who gives and gets the info?
b. Why do those parties need the info?
c. Under what restrictions is the info shared?

2. What information does the Offense needs from the Defense?
3. What information does the Defense needs from the Offense?
4. What type of information is to be shared?
5. What type of information is beneficial to each community?

~~SECRET//20330207~~

Next Steps:

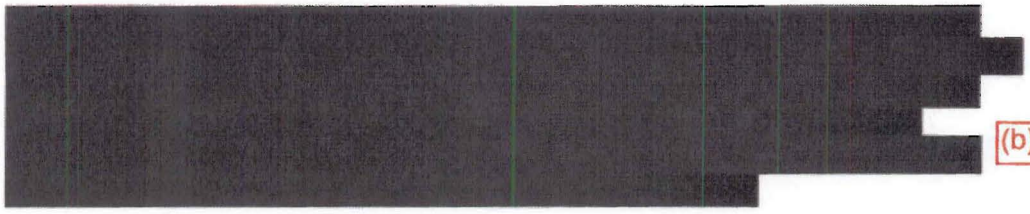
DOC 209
Release in Part (b)(3)

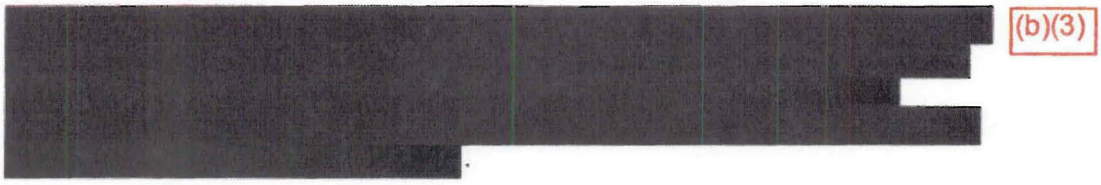
The United States has the right to take measures it deems necessary to protect national security interests and to prevent disclosure of classified and sensitive information.

Counterintelligence is one of several instruments of national power that can enact these necessary measures, but its effectiveness depends . . . on coordination with other elements of government and with the private sector.

This is even more important for cybersecurity activities, which can take many forms: defense (CND), offense (CNA), investigation (CNI), as well as counterintelligence (CI). These activities are all linked and properly coordinated can enable each other and close gaps an enemy might otherwise exploit.

Proper coordination should begin with a firm understanding of the "equities" involved and agreements on where equities lie for cybersecurity activities and stakeholders. By equities, we mean understood or claimed mission areas that, if rights and roles were not clarified, could result in uncoordinated or counter-productive actions.



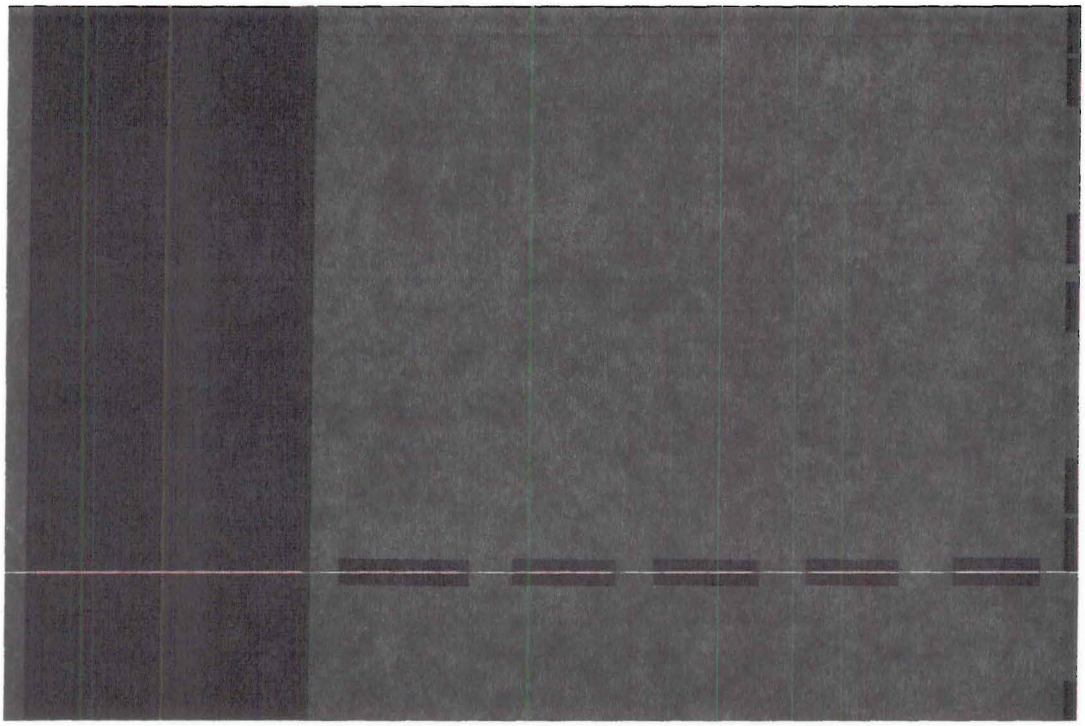


The Vulnerabilities Equities Process Working Group (VEPWG) has asked for drafting of scenarios (vignettes) that illustrate issues to be handled by a USG-wide vulnerabilities equities process. ONCIX has been tasked to provide examples of CI equities via one or more vignettes as well.

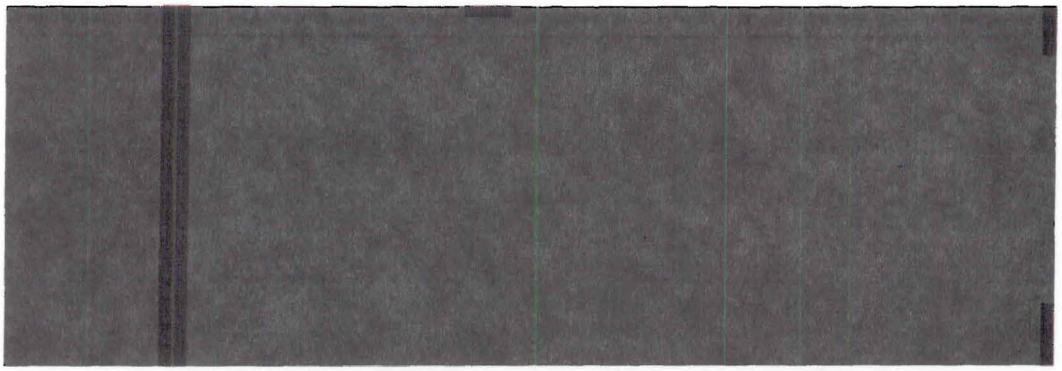
[redacted] (b)(1), (b)(3), (b)(5)

First, some definitions for those not familiar with the counterintelligence mission:

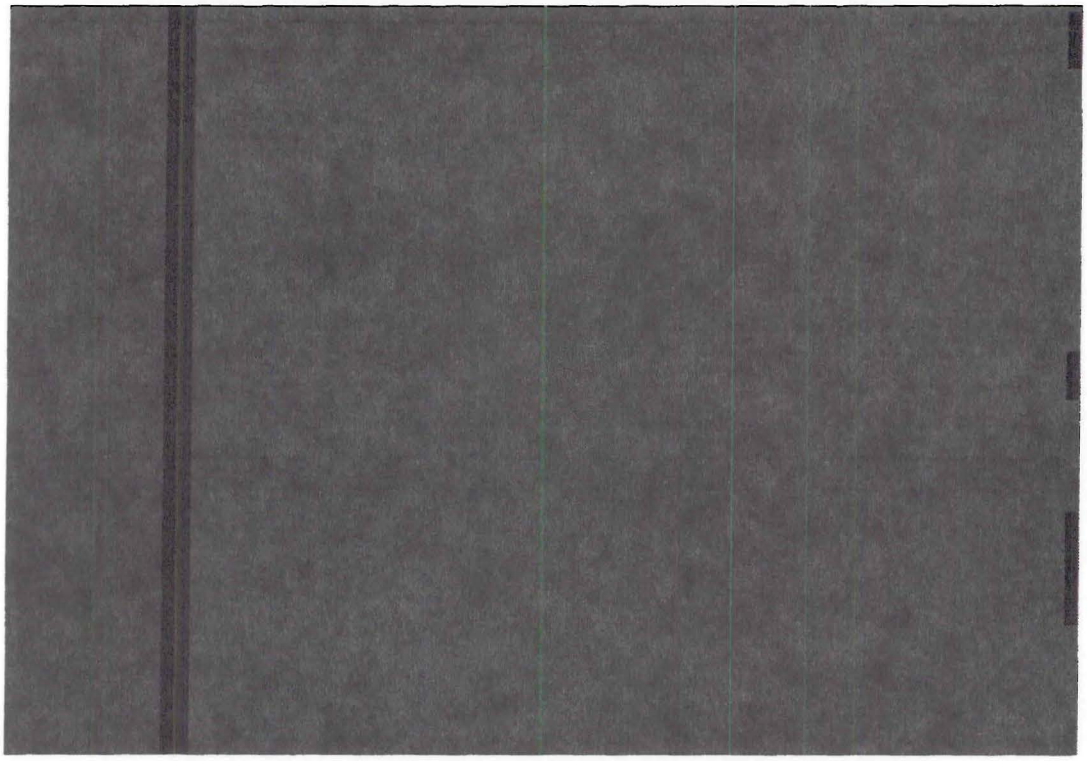
> **Counterintelligence**: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, foreign organizations or persons, or their agents, or international terrorist organizations or activities.



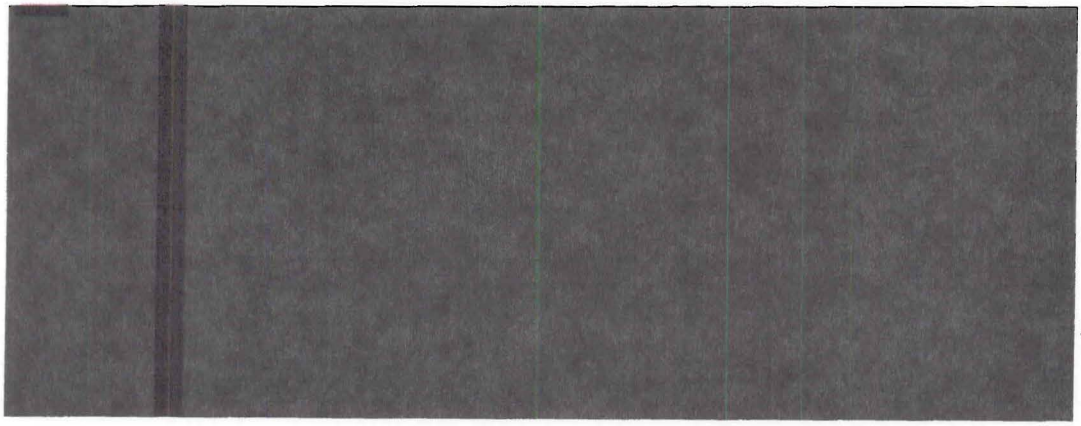
(b)(1), (b)(3), (b)(5)



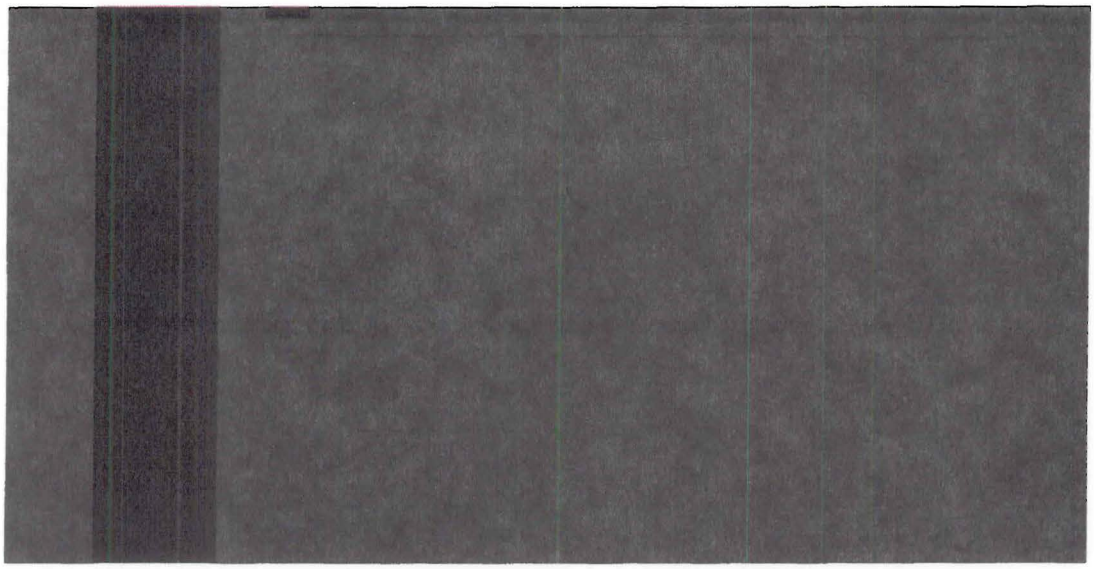
(b)(1), (b)(3), (b)(5)



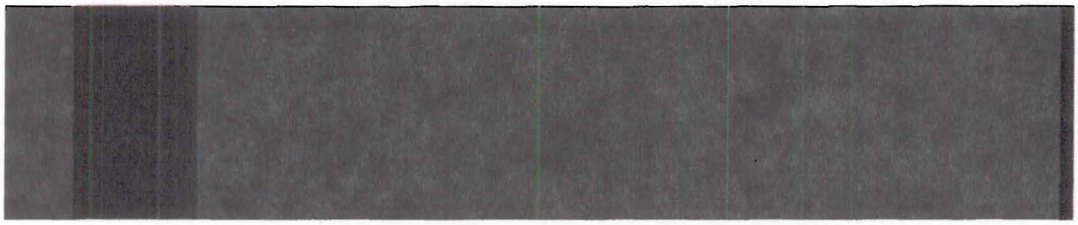
(b)(1), (b)(3), (b)(5)



(b)(1), (b)(3), (b)(5)



(b)(1), (b)(3), (b)(5)



(b)(1), (b)(3), (b)(5)