



**LIMITLESS SURVEILLANCE AT THE FDA:  
PROTECTING THE RIGHTS OF FEDERAL WHISTLEBLOWERS**

**JOINT STAFF REPORT**

**Prepared for**

**Representative Darrell E. Issa, Chairman  
Committee on Oversight and Government Reform  
United States House of Representatives**

**&**

**Senator Charles E. Grassley, Ranking Member  
Committee on the Judiciary  
United States Senate**

**113th Congress  
February 26, 2014**

---

# **I. Table of Contents**

---

<b>I.</b>	<b>Table of Contents</b> .....	2
<b>II.</b>	<b>Table of Names</b> .....	3
<b>III.</b>	<b>Executive Summary</b> .....	5
<b>IV.</b>	<b>Findings</b> .....	9
<b>V.</b>	<b>Recommendations</b> .....	11
<b>VI.</b>	<b>Background</b> .....	12
A.	Confidential Documents are Posted Online .....	16
<b>VII.</b>	<b>Authorization and Instructions for Monitoring</b> .....	17
<b>VIII.</b>	<b>Details of the Computer Monitoring</b> .....	25
<b>IX.</b>	<b>Evolution of the Monitoring Program</b> .....	29
B.	Initiation of Monitoring.....	29
C.	Type of Monitoring .....	31
D.	Development of Search Terms.....	32
E.	Interim Report .....	33
F.	Expansion of People Monitored .....	35
G.	Changes to the FDA Employee Login Disclaimer.....	35
<b>X.</b>	<b>The Office of Inspector General Declines to Investigate</b> .....	39
<b>XI.</b>	<b>Monitoring Was Not the Solution</b> .....	41
<b>XII.</b>	<b>Managing By Investigation</b> .....	42
<b>XIII.</b>	<b>Post-Monitoring Changes</b> .....	45
<b>XIV.</b>	<b>Conclusion</b> .....	47
<b>XV.</b>	<b>Appendix I: Relevant Documents</b> .....	49

---

## **II. Table of Names**

---

### **Food and Drug Administration**

#### **Jeffrey Shuren**

*Director, Center for Devices and Radiological Health*

Jeffrey Shuren is the Director for the Center for Devices and Radiological Health. He oversees the Center's operations and strategic direction. Dr. Shuren, along with several other FDA officials, ordered the initial computer monitoring and was a later proponent of its expansion.

#### **Ruth McKee**

*Associate Director for Management and Executive Officer, Center for Devices and Radiological Health*

Ruth McKee is the Associate Director for Management and Executive Officer for the Center for Devices and Radiological Health. McKee reports directly to Dr. Shuren, who tasked her to lead the charge to determine what steps the FDA needed to take after it learned of the potential leak. McKee also ordered the monitoring and determined the initial monitoring search terms given to the Office of Information Management.

#### **Mary Pastel**

*Deputy Director for Radiological Health for In Vitro Diagnostics, Center for Devices and Radiological Health*

Mary Pastel is the Deputy Director for Radiological Health for *In Vitro* Diagnostics with the Center for Devices and Radiological Health. Ruth McKee instructed Pastel to review encrypted flash drives containing surveillance of information on scientists' computers.

#### **Lori Davis**

*Chief Information Officer*

Lori Davis was the Chief Information Officer for the FDA. Prior to being named the Chief Information Officer in January 2009, she served as the Deputy Chief Information Officer. She worked with Ruth McKee to set up computer monitoring of Dr. Robert Smith, and was asked to search through e-mails of FDA employees to determine the source of the information leak.

#### **Joe Albaugh**

*Chief Information Security Officer*

Joe Albaugh was the Chief Information Security Officer for the FDA until March 2011. Lori Davis approached Albaugh to set up the computer monitoring for Dr. Robert Smith.

**Robert Smith**

*Medical Officer, Center for Devices and Radiological Health*

Robert Smith was a Medical Officer for the Center for Devices and Radiological Health. He was the first employee at the FDA to experience computer monitoring. Based on information gathered from Dr. Smith's computer, officials at the FDA later expanded this monitoring to include additional FDA scientists. His contract was not renewed after his contacts with Congress, the Office of Special Counsel, and his personal attorney were captured through the FDA's monitoring program.

**Les Weinstein**

*Ombudsman, Center for Devices and Radiological Health*

Les Weinstein was the Ombudsman in the Office of the Center Director for the Center for Devices and Radiological Health. Weinstein asked the U.S. Department of Health and Human Services Office of Inspector General to investigate the disclosure of confidential information to the press.

**Chickasaw Nation Industries Information Technology, LLC****Christopher Newsom**

*Contract Forensic Engineer, Incident Response Team*

Christopher Newsom is a Forensic Engineer with Chickasaw Nation Industries Information Technology. Newsom conducted the computer monitoring of FDA employees. After the FDA first set up this monitoring for Dr. Robert Smith, Newsom prepared an interim report to summarize the status of the monitoring.

**Joseph Hoofnagle**

*Contract Investigator, Incident Response Team*

Joseph Hoofnagle is a Contract Investigator with Chickasaw Nation Industries Information Technology. Hoofnagle installed Spector 360 software on the monitored employees' computers. He worked with Newsom to conduct computer monitoring of FDA employees, and assisted Newsom in writing an interim report to summarize the status of the monitoring.

---

### III. Executive Summary

---

In January 2009, several national news outlets, including the *New York Times*, *Associated Press*, and the *Wall Street Journal*, reported that U.S. Food and Drug Administration (FDA) scientists had lodged complaints that the agency was approving unsafe and risky medical devices.<sup>1</sup> In March 2010, the *New York Times* published a follow-up article reporting allegations by FDA scientists that the FDA ignored radiation warnings when approving certain medical devices.<sup>2</sup>

Specifically, Dr. Robert Smith and four other employees of the FDA's Center for Devices and Radiological Health (CDRH) expressed concern about FDA-approved medical devices. Dr. Smith believed FDA managers ignored warnings from scientists regarding potential health hazards related to radiation exposure. Dr. Smith and the other CDRH employees also expressed their concerns to Congress and the 2009 White House Transition Team.<sup>3</sup> Additionally, Dr. Smith and his colleagues reported allegations of retaliation to Congress and the U.S. Office of Special Counsel (OSC).<sup>4</sup>

Upon learning CDRH scientists publicly disclosed information about pending device applications, known as 510(k) applications, CDRH management initiated an electronic surveillance program of unprecedented scope. To determine which scientists were disclosing information and what specific information they were disclosing, the CDRH engaged two contractors working on the FDA's information technology security systems in April 2010 to begin monitoring Dr. Smith.<sup>5</sup> Approximately one month later, the monitoring expanded to another CDRH scientist.<sup>6</sup> Using a software monitoring program called Spector 360, which took screenshots of FDA employees' computers every five seconds,<sup>7</sup> FDA officials were able to obtain sensitive information and protected communications, including attorney-client

---

<sup>1</sup> Gardiner Harris, *In F.D.A. Files, Claims of Rush to Approve Devices*, N.Y. TIMES, Jan. 13, 2009, available at [http://www.nytimes.com/2009/01/13/health/policy/13fda.html?\\_r=0](http://www.nytimes.com/2009/01/13/health/policy/13fda.html?_r=0) (last visited Feb. 21, 2014) [hereinafter *Rush to Approve Devices*]; Ricardo Alonso-Zaldivar, *FDA Scientists Complain to Obama of 'Corruption,'* ASSOC. PRESS, Jan. 8, 2009 [hereinafter *Scientists Complain to Obama*]; Alicia Mundy & Jared Favole, *FDA Scientists Ask Obama to Restructure Drug Agency*, WALL ST. J., Jan. 8, 2009, available at <http://online.wsj.com/news/articles/SB123142562104564381> (last visited Feb. 21, 2014).

<sup>2</sup> Gardiner Harris, *Scientists Say F.D.A. Ignored Radiation Warnings*, N.Y. TIMES, Mar. 28, 2010, available at <http://www.nytimes.com/2010/03/29/health/policy/29fda.html?pagewanted=all> (last visited Feb. 21, 2014) [hereinafter *F.D.A. Ignored Radiation Warnings*].

<sup>3</sup> *Scientists Complain to Obama*, *supra* note 1.

<sup>4</sup> Letter from Lindsey M. Williams, Dir. of Advocacy & Dev., Nat'l Whistleblowers Ctr., to Sen. Chuck Grassley, Ranking Member, Senate Judiciary Comm., Chairman Darrell Issa, H. Comm. on Oversight & Gov't Reform, & Special Counsel Carolyn Lerner, U.S. Office of Special Counsel (Sept. 17, 2012) [hereinafter *NWC Letter*]; Letter from CDRH Scientists, Office of Device Evaluation, Food & Drug Admin. (FDA), to Rep. John Dingell, U.S. House of Representatives (Oct. 14, 2008) [hereinafter *CDRH Letter*].

<sup>5</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Ruth McKee, at 7-9 (Nov. 13, 2012) [hereinafter *McKee Tr.*].

<sup>6</sup> See Letter from Jeanne Ireland, Ass't Comm'r for Legis., FDA, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight and Gov't Reform (July 13, 2012) [hereinafter *Ireland Letter*].

<sup>7</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Christopher Newsom, at 10-11 (Oct. 2, 2012) [hereinafter *Newsom Tr.*].

communications, communications with Congress, and communications with the OSC. The FDA intercepted communications with congressional staffers and draft versions of whistleblower complaints complete with editing notes in the margins.<sup>8</sup> The agency also took electronic snapshots of the computer desktops of the FDA employees and reviewed documents and files they saved on the hard drives of their government computers as well as personal thumb drives attached to their computers.<sup>9</sup> FDA even reconstructed files that had been deleted from personal thumb drives prior to the device being used on an FDA computer.

The contractors conducting the investigation prepared an interim report to update FDA officials.<sup>10</sup> This report, which was sent to Deputy Chief Information Officer Lori Davis on June 3, 2010, attempted—yet could not definitively support—a link to Dr. Smith with the release of 510(k) information to non-FDA employees.<sup>11</sup> The report described information found on Dr. Smith’s computer, including e-mails with journalists, Congress, and the Project on Government Oversight.<sup>12</sup> The report also stated that Dr. Smith “ghostwrote” reports for his subordinates and supplied internal CDRH documents to external sources.<sup>13</sup> After receiving this report, the FDA expanded the computer monitoring to include three additional CDRH scientists<sup>14</sup> and declined to renew Dr. Smith’s contract.<sup>15</sup>

FDA officials also contacted the Department of Health and Human Services (HHS) Office of Inspector General (OIG) on numerous occasions to request an investigation into the disclosures.<sup>16</sup> The OIG declined these requests, noting that contacts with the media and Congress were lawful, and no evidence of criminal conduct existed.<sup>17</sup> Despite the OIG’s repeated refusal to investigate, the FDA continued to monitor Dr. Smith and his colleagues in the hope of finding enough evidence to convince the OIG to take action.<sup>18</sup> However, the FDA failed to take direct administrative or management action on its own to address the concerns directly.

---

<sup>8</sup> Ellen Nakashima and Lisa Rein, *FDA staffers sue agency over surveillance of personal e-mail*, WASH. POST, Jan. 29, 2012.

<sup>9</sup> *Id.*

<sup>10</sup> Memorandum from Joseph Hoofnagle, Incident Response & Forensic Lead & Christopher Newsom, Incident Response & Forensic Investigator, *Interim Report of Investigation – Robert C. Smith* (June 3, 2010) [hereinafter Interim Report].

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> McKee Tr. at 16.

<sup>15</sup> *Id.* at 33.

<sup>16</sup> Letter from Jeffrey Shuren, Dir., Ctr. for Devices & Radiological Health, FDA, to Daniel R. Levinson, Inspector Gen., Dep’t of Health & Human Servs. (Feb. 23, 2011) [hereinafter Shuren Letter, Feb. 23, 2011]; Letter from Les Weinstein, Ombudsman, Center for Devices & Radiological Health (CDRH), FDA, to Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., U.S. Dep’t of Health & Human Servs. (HHS) (Mar. 23, 2009); E-mail from Les Weinstein, Ombudsman, CDRH, FDA, to Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., HHS (Oct. 23, 2009, 6:06 p.m.) [hereinafter Weinstein E-mail].

<sup>17</sup> Letter from Scott A. Vantrease, Asst. Special Agent in Charge, Special Investigations Branch, Office of the Inspector Gen., HHS, to Mark McCormack, Special Agent in Charge, Office of Criminal Investigations, Office of Internal Affairs, FDA (May 18, 2010) [hereinafter Vantrease Letter].

<sup>18</sup> H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Jeffrey Shuren, at 20-21 (Nov. 30, 2012) [hereinafter Shuren Tr.].

FDA officials eventually forwarded information gathered from the computer monitoring program to the OIG.<sup>19</sup> The OIG contacted the Criminal Division of the Department of Justice to determine whether the evidence collected by the FDA against Dr. Smith and his colleagues supported a criminal referral.<sup>20</sup> In November 2010, by letter, the Criminal Division formally declined to take up the matter.<sup>21</sup>

FDA's overly-invasive monitoring program came to light in January 2012, when Dr. Smith and several of his colleagues filed a lawsuit in U.S. District Court in Washington, D.C. The suit alleged that information gathered during the monitoring was used to harass or dismiss at least six current and former FDA employees. House Committee on Oversight and Government Reform Chairman Darrell Issa and Senate Committee on the Judiciary Ranking Member Charles Grassley (the Committees) subsequently launched a joint investigation into the monitoring program.

In May 2012, documents associated with the monitoring were posted on a public internet site. Included in these materials were confidential and proprietary FDA documents, as well as confidential communications between FDA employees and Congress, the OSC, and personal attorneys.<sup>22</sup>

Witnesses who contacted the Committees voiced concerns about the intrusive nature of the surveillance, and the irresponsibility in posting the fruits of the surveillance on the Internet for anyone to see. They believed that the FDA conducted surveillance for the sole purpose of retaliating against the scientists for raising concerns about the medical device review process.

The Committees conducted seven transcribed interviews with current and former FDA employees and contractors and reviewed approximately 70,000 documents. The pace of the Committees' investigation was slowed by FDA's unwillingness to cooperate. The FDA repeatedly cited the ongoing litigation with Dr. Smith and his colleagues as an excuse to withhold documents and information.

Documents and information obtained by the Committees show the FDA conducted this monitoring program without regard for employees' rights to communicate with Congress, the OSC, or their personal attorneys. The Committees' investigation also found that data collected could be used to justify adverse personnel actions against agency whistleblowers. Absent a lawful purpose, an agency should not conduct such invasive monitoring of employees' computer activity. The FDA failed not only to manage the monitoring program responsibly, but also to consider any potential legal limits on its authority to conduct surveillance of its employees. The Committees' investigation has shown that agencies need clearer policies addressing appropriate monitoring practices to ensure that agency officials do not order or conduct surveillance beyond their legal authority or in order to retaliate against whistleblowers, especially in such a way that

---

<sup>19</sup> Letter from Jeffrey Shuren, Dir., Ctr. for Devices & Radiological Health, FDA, to Hon. Daniel Levinson, Inspector Gen., Dep't of Health & Human Servs. (June 28, 2010) [hereinafter Shuren Letter, June 28, 2010].

<sup>20</sup> Shuren Tr. at 67-68.

<sup>21</sup> Letter from Jack Smith, Chief, Public Integrity Section, Dep't of Justice, to David Mehring, Special Agent, Office of the Inspector Gen., Dep't of Health & Human Servs. (Nov. 3, 2010) [hereinafter DOJ Letter].

<sup>22</sup> *Id.*

chills whistleblower communications with Congress, the OSC, and Inspectors General.<sup>23</sup> Congress has a strong interest in keeping such lines of communication open, primarily as a deterrent to waste, fraud, and abuse in Executive Branch departments and agencies.

Whistleblower disclosures are protected by law, even if they are ultimately unsubstantiated, so long as the disclosure was made in good faith. Accordingly, the analysis of the issues examined in this report is not dependent on the merits of the underlying claims that whistleblowers made about the safety of certain medical devices. Thus, this report does not examine the merits of those underlying claims and takes no position on whether the devices in question posed a risk to public health.

---

<sup>23</sup> The Whistleblower Protection Act provides protections for whistleblowers against personnel actions taken because of a protected disclosure made by a covered employee. The Act provides that “any disclosure of information” made by a covered employee who “reasonably believes” evidences “a violation of any law, rule, or regulation” or evidences “gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety” so long as the disclosure is not prohibited by law nor required to be kept secret by Executive Order. *See* 5 U.S.C. § 2302(b)(8)(A); Cong. Research Serv., Whistleblower Protection Act: An Overview, at 3 (Mar. 12, 2007), *available at* <http://www.fas.org/sgp/crs/natsec/RL33918.pdf> (last visited Feb. 21, 2014).

---

## IV. Findings

---

- CDRH scientists and doctors raised concerns to Congress, the OSC, and President Obama’s transition team about pressure from management to approve medical devices they believed were unsafe.
- Despite the extensive scope of the monitoring, there was insufficient written authorization, no monitoring policy in place, and there was no legal guidance given to the contractors who conducted the monitoring. The lack of any legal guidance to limit the monitoring program resulted in FDA capturing protected communications.
- Although FDA claimed to be investigating a specific leak of 510(k) information, the computer monitoring did not include a retrospective inquiry into any of the scientists’ network activities. When interviewed, FDA managers and IT professionals failed to explain clearly how the rationale offered to justify the monitoring (investigating a past leak) was consistent with the method used (monitoring current activity). The goal of monitoring was allegedly to identify who leaked confidential information. Instead of looking back at previous communications using available tools in their possession, however, the FDA chose real-time monitoring of current and future communications. Because FDA managers lacked formal investigative training and did not understand the legal concerns related to employee monitoring, they believed all employee communications that occurred on government computers were “fair game.”
- Because FDA managers lacked formal investigative training and legal guidance, they did not understand the legal limits of permissible employee monitoring. As a result, the scope was limited only by the FDA’s technical capabilities. For example, those conducting the monitoring said they believed all employee activity having any remote nexus to government computers was “fair game”—even to the point of forensically recovering deleted files from personal storage devices when plugged into FDA computers. Moreover, the monitoring software collected all keystrokes on the computers, including the passwords for personal email accounts and online banking applications, even though *de minimis* personal use is permitted.
- The monitoring program began when a law firm representing a manufacturer alleged unlawful disclosures were made to the press regarding a device that was under FDA review. Ruth McKee first ordered monitoring on Dr. Smith’s computer because Dr. Smith was believed to be the source of the leak. Later, monitoring expanded to include four additional CDRH scientists. Officials used Spector 360, a software package that recorded user activity with powerful capture and analysis functions, including real-time surveillance and keystroke logging.
- The FDA’s surveillance was not lawful, to the extent that it monitored communications with Congress and the Office of Special Counsel. Federal law protects disclosures to OSC and Congress.

- HHS OIG denied FDA's repeated requests for an OIG investigation into the allegedly wrongful disclosures. OIG found no evidence of criminal conduct on the part of any employee. Still, officials continued to contact OIG to request an investigation. OIG again denied the request, and the Justice Department declined to take action.
- The monitoring program ultimately failed to identify who leaked information to the *New York Times* or the *Wall Street Journal*, despite capturing approximately 80,000 documents and inadvertently publishing those documents on the Internet.
- Despite known complaints about performance issues regarding Dr. Robert Smith, FDA management and leadership chose to address Dr. Smith's employment status through repeated requests for criminal investigation, rather than by simply taking administrative or managerial actions directly within its own control and authority.
- Over a year after receiving directives from OMB, OSC, and the FDA Commissioner, the FDA produced interim guidelines on monitoring procedures in September 2013. The FDA's interim policies require written authorization prior to initiating employee monitoring. Only the Commissioner, Deputy Commissioner, or the Chief Operating Officer can authorize surveillance of employees. The FDA has not yet implemented permanent policies to govern employee monitoring.
- The FDA's interim policies do not provide safeguards to protect whistleblowers from retaliation. Under these policies, protected communications are still subject to monitoring and may be viewed by agency officials.

---

## V. Recommendations

---

Based on its investigation, the Committees identified several recommendations that, if implemented, would assist other Executive Branch departments and agencies in avoiding a repeat of the mistakes made by the FDA:

- The FDA should promptly develop permanent written procedures to govern employee monitoring and safeguard protected communications through substantive restrictions on the scope of surveillance that can be authorized on employees. Procedural safeguards merely requiring approval of surveillance by senior officials are not enough.
- The FDA should ensure that programs used to monitor employees do not collect personal information such as bank account numbers or passwords for personal e-mail accounts.
- The FDA's interim guidance does not include provisions to protect employees against retaliation if communications with Congress, the OSC, or personal attorneys are captured through monitoring. The FDA should establish procedures that ensure protected whistleblower communications cannot be used for retaliation.
- The FDA should develop clear guidance for identifying and filtering protected communications so that protected communications are not retained or shared for any reason. Any employee or contractor involved in the monitoring process, including the Review Committee established by the September 26, 2013 Staff Manual Guide, should be trained on these procedures.
- Employees should be notified that their communications with Congress and the OSC are protected by law.
- The OSC should modify its June 20, 2012 memorandum to all federal agencies regarding monitoring policies to include communications with Congress.<sup>24</sup>
- The GAO should conduct a study of all Executive Branch departments and agencies to determine whether the guidelines set forth for computer monitoring in the OSC's June 20, 2012 memorandum have been implemented.

---

<sup>24</sup> Memorandum from Carolyn Lerner, Special Counsel, U.S. Office of Special Counsel to Executive Branch Departments and Agencies, *Agency Monitoring Policies & Confidential Whistleblower Disclosures to the Office of Special Counsel & to Inspectors General* (June 20, 2012) [hereinafter Lerner Memo].

---

## VI. Background

---

**FINDING:** CDRH scientists and doctors raised concerns to Congress, the OSC, and President Obama’s transition team about pressure from management to approve medical devices they believed were unsafe.

The Food and Drug Administration (FDA), a component of the U.S. Department of Health and Human Services (HHS), is responsible for promoting public health.<sup>25</sup> Specifically, the FDA is charged with regulating and supervising a variety of consumer health products.<sup>26</sup> These products include dietary supplements, prescription and over-the-counter drugs, vaccines, biopharmaceuticals, and medical devices.<sup>27</sup> The FDA has broad powers for determining the safety, risks, marketing, advertising, and labeling of these products.<sup>28</sup>

The Center for Devices and Radiological Health (CDRH) is a division within the FDA.<sup>29</sup> The CDRH is also tasked with protecting and promoting public health.<sup>30</sup> The mission of the CDRH is to ensure that patients and providers of health services have access to safe medical devices, such as hip implants, heart valves, and mammography machines.<sup>31</sup> The CDRH tests and examines potential medical devices, and makes recommendations to the FDA regarding the approval and widespread usage of radiation-emitting products.<sup>32</sup> The CDRH seeks to assure consumer confidence in devices manufactured in the United States.<sup>33</sup> Scientists and doctors who work for the CDRH are directly involved in product testing, making recommendations to the FDA, and assessing whether the medical devices are safe for public use.<sup>34</sup>

In 2007, CDRH scientists first started raising concerns about the FDA’s marketing of unsafe medical devices used to detect cancers of the breast and colon.<sup>35</sup> These scientists also complained of a toxic work environment in which they feared retaliation by their managers for writing unsupportive reviews of medical devices they believed to be unsafe.<sup>36</sup> The scientists argued that the CDRH’s process for approving medical devices for public use was not sufficiently rigorous and that the FDA’s premature release of products without sufficient testing posed health risks to the public.<sup>37</sup> In an attempt to implement more stringent guidelines for this

---

<sup>25</sup> FDA, *About FDA*, <http://www.fda.gov/AboutFDA/default.htm> (last visited Feb. 21, 2014).

<sup>26</sup> FDA, *About FDA: What Does FDA Regulate?*, <http://www.fda.gov/aboutfda/transparency/basics/ucm194879.htm> (last visited Feb. 21, 2014).

<sup>27</sup> *Id.*

<sup>28</sup> FDA, *About FDA: What Does FDA Do?*, <http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194877.htm> (last visited Feb. 21, 2014).

<sup>29</sup> FDA, *Training & Continuing Education: CDRH Learn*, <http://www.fda.gov/Training/CDRHLearn/default.htm> (last visited Feb. 21, 2014).

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> FDA, *About FDA: CDRH Mission, Vision & Shared Values*, <http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/ucm300639.htm> (last visited Feb. 21, 2014).

<sup>34</sup> *Id.*

<sup>35</sup> CDRH Letter, *supra* note 4.

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

testing process, the CDRH scientists filed complaints with the OSC,<sup>38</sup> the HHS OIG, Congress,<sup>39</sup> and even the transition team for then-President-elect Obama.<sup>40</sup>

On January 13, 2009, the *New York Times* published an article stating that “front-line agency scientists believed that FDA managers [had] become too lenient with the industry.”<sup>41</sup> The article further stated that “an agency supervisor improperly forced them to alter reviews of [a] breast imaging device.”<sup>42</sup> The article, citing internal FDA documents, referred specifically to the ongoing review of the iCAD SecondLook Digital Computer-Aided Detection System for Mammography device.<sup>43</sup> The article further stated:

One extensive memorandum argued that FDA managers had encouraged agency reviewers to use the abbreviated process even to approve devices that are so complex or novel that extensive clinical trials should be required. An internal review said the risks of the iCAD device included missed cancers, “unnecessary biopsy or even surgery (by placing false positive marks) and unnecessary additional radiation.”<sup>44</sup>

Later that day, Ken Ferry, the Chief Executive Officer of iCAD, wrote a letter to the CDRH Ombudsman, Les Weinstein, urging him to look into the breach of confidentiality concerning the pre-market approval of iCAD’s breast-imaging device.<sup>45</sup> Ferry reminded the Ombudsman that the FDA cannot release confidential information submitted to the FDA as part of a premarket approval application, including any supplements to the application, without

---

<sup>38</sup> The U.S. Office of Special Counsel is the first step in the whistleblower review process. OSC is an independent federal investigative and prosecutorial agency. Its primary goal is to safeguard all protected employees from prohibited personnel practices, especially reprisal for whistleblowers. U.S. Office of Special Counsel, *Introduction to OSC*, <http://www.osc.gov/Intro.htm> (last visited Feb. 21, 2014); NWC Letter, *supra* note 4; CDRH Letter, *supra* note 4.

<sup>39</sup> Employees who provide information to Congress are protected by the Whistleblower Protection Act (WPA). See 5 U.S.C. § 7211. The WPA provides statutory protections for federal employees who make disclosures reporting illegal or improper activities, including employees who provide information to Congress. See *id.*; Eric A. Fischer, Cong. Research Serv., *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, at 16 (June 20, 2013) (“A reasonable argument could be made that monitoring the content of every employee communication is excessively intrusive.”). Additionally, the Fourth Amendment protects individuals from unreasonable searches and seizures. U.S. CONST. Amend. IV. states, in pertinent part: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” The Supreme Court recognizes individuals do not lose Fourth Amendment rights merely because they work for the government as opposed to a private employer. See *City of Ontario v. Quon*, 560 U.S. 746; 130 S. Ct. 2619 (2010).

<sup>40</sup> CDRH Letter, *supra* note 4; NWC Letter, *supra* note **Error! Bookmark not defined.**4; Telephone Call with Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., HHS (May 26, 2009); Letter from CDRH Scientists, CDRH, FDA, to John D. Podesta, Presidential Transition Team (Jan. 7, 2009).

<sup>41</sup> *Rush to Approve Devices*, *supra* note 1.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> Letter from Ken Ferry, Pres. & Chief Exec. Officer, iCAD, to Les Weinstein, Ombudsman, CDRH, FDA (Jan. 13, 2009) [hereinafter Ferry Letter].

explicit permission.<sup>46</sup> Rather than taking any steps to deal with the issue directly, CDRH managers forwarded the complaint to the OIG.<sup>47</sup>

Ferry also noted that a *New York Times* reporter had called him four days before the article was published.<sup>48</sup> The reporter had questions concerning an internal dispute at the CDRH, which was reviewing iCAD's application.<sup>49</sup> According to Ferry's letter, the reporter told Ferry that the proprietary documents "were sent [to the reporter] by Scientific Officers of the FDA."<sup>50</sup>

On October 1, 2009, Dr. Jeffrey Shuren, Director of the CDRH, talked to a reporter about a different medical device.<sup>51</sup> Dr. Shuren learned that the reporter was also in possession of similar documents related to the pre-market medical device process.<sup>52</sup> To better understand who may have provided the information, the CDRH asked its IT Department to compile a list of those scientists that accessed a certain working memo that would either approve or reject the device under review.<sup>53</sup>

---

<sup>46</sup> *Id.*

<sup>47</sup> Memorandum from Les Weinstein, Ombudsman, CDRH, FDA, *Documents Related to the Radiological Devices Branch* (Mar. 23, 2009).

<sup>48</sup> Ferry Letter, *supra* note 45.

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> Weinstein E-mail, *supra* note 16.

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

Shuren, Jeff

From: Weinstein, Les S  
Sent: Friday, October 23, 2009 6:06 PM  
To: [REDACTED]  
Cc: Shuren, Jeff  
Subject: Unauthorized Disclosures

Attachments: Document.pdf; K083191 audit.xls; NYT Jan 13 2009.pdf; K071871 – clinical cardiology review LEWIS March 26 2008.doc; Document.pdf; Document.pdf

To get a list of people who electronically accessed the memo, we asked our IT staff to search IMAGE audit information from the date of the memo (April 9) up to and including the date of the interview with Ms. Mundy (October 1). The following list shows that four people accessed the 25-page document indicated by the color green in column . The color yellow indicates a related 2-page document that is fully disclosable; I am not attaching this document.)



K083191 audit.xls  
(20 KB)

Les Weinstein  
Ombudsman  
Office of the Center Director  
Center for Devices and Radiological Health  
Food and Drug Administration

**“To get a list of people who electronically accessed the memo, we asked our IT staff to search IMAGE audit information . . . .”**

CDRH officials forwarded four names resulting from this search to the Office of Inspector General.<sup>54</sup> Dr. Shuren testified that he “did not recall” if the OIG was going to look into the matter.<sup>55</sup>

On March 28, 2010, the *New York Times* published a second article regarding the FDA’s approval process for medical devices.<sup>56</sup> This second article, published fourteen months after the January 2009 article, cited information concerning a GE Healthcare device under FDA review:

Scores of internal agency documents made available to The New York Times show that **agency managers sought to approve an application by General Electric to allow the use of CT scans for colon cancer screenings over the repeated objections of agency scientists**, who wanted the application rejected. It is still under review.<sup>57</sup>

On April 16, 2010, GE Healthcare’s outside legal counsel wrote to Dr. Shuren to request an internal investigation and a meeting to discuss a possible breach of confidentiality regarding GE Healthcare’s device under FDA review.<sup>58</sup> The letter stated:

GE Healthcare is extremely concerned about this violation of confidentiality and respectfully requests that you conduct an internal investigation into how this information was leaked to the press.<sup>59</sup>

<sup>54</sup> *Id.*

<sup>55</sup> Shuren Tr. at 14.

<sup>56</sup> *F.D.A. Ignored Radiation Warnings*, *supra* note 2.

<sup>57</sup> *Id.* (emphasis added).

<sup>58</sup> Letter from Edward M. Basile, Partner, King & Spalding LLP, to Jeffrey E. Shuren, Dir., CDRH, FDA (Apr. 16, 2010) [hereinafter Basile Letter].

In light of the two *New York Times* articles describing internal turmoil at the FDA, as well as complaints filed by both iCAD and GE Healthcare, the FDA began real-time monitoring of CDRH employees' computer activity.

### ***A. Confidential Documents are Posted Online***

In May 2012, an HHS contractor, Quality Associates, Inc (QAI), posted approximately 80,000 pages of documents associated with the FDA employee monitoring on a public internet site.<sup>60</sup> Included in these materials were confidential and proprietary FDA documents, as well as confidential communications between FDA employees and Congress, OSC, and personal attorneys.<sup>61</sup> FDA had asked the HHS Program Support Center (PSC) to use a contractor to produce and print PDF-versions of the surveillance records, and PSC tasked contractor QAI with the project.<sup>62</sup>

After the documents left FDA, they followed a chain of custody that included several parties before they got to QAI.<sup>63</sup> According to HHS, QAI received the job from PSC on May 2, 2012, and completed it on May 9, 2012.<sup>64</sup> The files were uploaded to the site at the direction of PSC, on May 3, 2012.<sup>65</sup> They were removed from the site and archived six days later on May 9, 2012.<sup>66</sup> During this time, confidential and proprietary information was publically available and easily searchable.<sup>67</sup>

QAI officials claimed they were simply following their client's instructions.<sup>68</sup> In fact, FDA did not mark the documents as confidential, and there is no written record reflecting the sensitive nature of the documents.<sup>69</sup> Furthermore, the purchase order, which was submitted to the Government Printing Office (GPO) only after the work was completed, failed to mention any sensitive classification.<sup>70</sup> When prompted on the purchasing order form, PSC checked the "no" boxes, indicating there was 1) no personally identifiable information (PII), 2) no classified information, and 3) no sensitive but unclassified (SBU) information contained in the files.<sup>71</sup> HHS identified the misclassification as a "clerical error at the PSC."<sup>72</sup>

---

<sup>59</sup> *Id.*

<sup>60</sup> Letter from Jim R. Esquea, Assistant Sec'y for Legis., U.S. Dep't of Health & Human Servs., to Hon. Charles E. Grassley, Ranking Member, S. Comm. on Judiciary (March 13, 2013) [hereinafter Esquea Letter].

<sup>61</sup> NWC Letter, *supra* note 4.

<sup>62</sup> Esquea Letter, *supra* note 60.

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

<sup>65</sup> Letter from Paul Swidersky, President, CEO, Quality Associates Inc., to Hon. Charles E. Grassley, Ranking Member, S. Comm. on Judiciary (July 17, 2012).

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *See id.*; *see also* Esquea Letter, *supra* note 60.

<sup>70</sup> DHHS, FDA, *GPO Simplified Purchase Agreement Work Order Form 4044* (May 23, 2012).

<sup>71</sup> *Id.*

<sup>72</sup> Esquea Letter, *supra* note 60.

FDA did not take responsibility for the mishandling of the documents.<sup>73</sup> Rather, FDA shifted the responsibility to HHS, which, in turn, attempted to blame QAI:

The PSC advised QAI that the documents were sensitive and that access to them should be limited. The PSC further requested that QAI delete all files on its computers after completing the job, and shred any printed documents in its possession. Regrettably, despite these instructions, QAI's unauthorized use of an unsecure website caused QAI to lose control of the confidential material.<sup>74</sup>

FDA and HHS refused to take responsibility for the mishandling, even though they failed to identify the documents as sensitive or confidential in the paperwork provided to the contractor. This raises doubt about the veracity of the claim that the agencies had notified QAI of the sensitive nature of the documents. The incorrect purchase order that was submitted to GPO was dubbed by HHS as “erroneous” and was prepared after the project’s completion.<sup>75</sup> HHS also pointed to shortcomings in the GPO form itself:

Unfortunately, the GPO's required Work Order forms do not reflect the variety of confidential material frequently handled by Executive Branch agencies, including material as to which Congress has imposed specific statutory protections. The forms provide only three document category options[.] . . . Other options for identifying protected information, such as confidential commercial information, are not available on GPO's Work Order form.<sup>76</sup>

However, the documents clearly contained personally identifiable information, and yet the form incorrectly indicated that there was no such information.

---

## VII. Authorization and Instructions for Monitoring

---

<b>FINDING:</b>	Despite the extensive scope of the monitoring, there was insufficient written authorization, no monitoring policy in place, and there was no legal guidance given to the contractors who conducted the monitoring. The lack of well-understood contours for the monitoring program caused the FDA to capture protected communications.
-----------------	--

---

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

**FINDING:** Despite the fact that FDA claimed to be investigating a specific leak of 510(k) information, the computer monitoring did not include a retrospective inquiry into any of the scientists' network activities. When interviewed, FDA managers and IT professionals failed to explain clearly how the rationale offered to justify the monitoring (investigating a past leak) was consistent with the method used (monitoring current activity).

On April 16, 2010, Ruth McKee, Executive Officer for the CDRH, approached Dr. Jeffrey Shuren, Director of the CDRH, concerning the April 2010 letter and asking him what to do. Dr. Shuren testified:

Q. And so how did you begin to look into the disclosure that appeared in the *New York Times*?

A. Well, I asked Ruth McKee, who is my Executive Officer, were there ways in which we could identify the source of the leak, a little bit akin to what happened in October, **is there something you can sort of look for to then support for doing an investigation.** One of the challenges we also faced at the center is that normally in the past, the Office of Internal Affairs would take it, they would look into it over concerns, at least to my understanding, over interventions from Senator Grassley over concerns about the Office of Internal Affairs investigating whistleblowers. The Commissioner had previously instructed the Office of Internal Affairs not to conduct investigations, I think particularly if there was any possible criminal conduct as [it] relates to employees who had allegations against the agency. So—and a copy was also given of the complaint to the Office of Internal Affairs. They subsequently sent that to the OIG as well.<sup>77</sup>

Dr. Shuren testified that in his conversation with McKee, he learned that FDA Chief Information Officer Lori Davis had authorized the monitoring:

A. [Ruth] wound up talking to the Chief Information Officer and then **told me afterwards that the Chief Information Officer had authorized computer monitoring,** thought it was serious and this was the step that should be taken.

Q. Was computer monitoring something that you had suggested to Ruth?

A. No.

---

<sup>77</sup> Shuren Tr. at 19-20 (emphasis added).

Q. You asked her to explore the options, and she came back with computer monitoring?

A. Not even from the option. **She spoke to Lori, and Lori authorized the monitoring. I will say that knowing of it, though, I didn't object to the monitoring.** I am not the expert for what are the circumstances to monitor a person's computer.<sup>78</sup>

Lori Davis, however, remembered the authorization of computer monitoring differently. She testified:

A. Well, we got the request from the center. I mean, asking on behalf of the center, the center asked, "Can you do that?"

Q. You mean Ruth runs the center?

A. Yes. **Ruth said, "Can you?" And we said, "Yes, we can."** So in my mind that was the authorization to proceed based [on] some conversation that obviously CDRH, whether or not that was Ruth or anybody else, I don't know, had with Joe Albaugh and either, you know, his staff at this point. I am assuming it's either Chris or Joe. Those conversations happened and they agreed on a course of action.

Q. **There was no written authorization?**

A. **Not that I'm aware of no.**<sup>79</sup>

Davis further testified that she told McKee that she would forward the request for monitoring to FDA Chief Information Security Officer Joe Albaugh, who would be able to set up the monitoring.<sup>80</sup> For his part, Albaugh testified that he was only "a pass through between the technical team that was within [his] division and the request of the CIO and the Executive Officer."<sup>81</sup>

The CDRH engaged two primary investigators, Joseph Hoofnagle and Christopher Newsom, who were in place to work on the FDA's information technology security systems contract with Chickasaw Nation Industries Information Technology (CNIIT), to ultimately lead the computer monitoring effort.<sup>82</sup>

---

<sup>78</sup> *Id.* at 21 (emphasis added).

<sup>79</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Lori Davis, at 17 (Jan. 8, 2013) (emphasis added) [hereinafter Davis Tr.].

<sup>80</sup> *Id.* at 9-10.

<sup>81</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Joe Albaugh, at 9 (Mar. 7, 2013) (emphasis added) [hereinafter Albaugh Tr.].

<sup>82</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Joseph Hoofnagle, at 6-7 (Oct. 11, 2012) [hereinafter Hoofnagle Tr.]; Newsom Tr. at 6-9.

Hoofnagle, a Contract Investigator with CNIIT who managed the Incident Response Team for the FDA's network security systems, received few instructions as to the extent of monitoring CDRH officials sought.<sup>83</sup> Hoofnagle's only instructions were to find documents that contained certain key words, including the letter K followed by specific numbers; such documents, which reflect the FDA's naming convention for 510(k) applications, were leaked to the press.<sup>84</sup> As a result, he created an initial document that would govern the investigation.<sup>85</sup>

Laptop Name - DRL0098686

Spector Client: installed and active since 4/22/10

SUBJECT: Robert C. Smith (RCS)  
Medical Officer  
WO66 RM0319G HFZ-470  
CDRH - ODE/DRARD

Search Terms:  
Colonography - SUBJECT feels the FDA is not handling this issue well.

Allegations:  
Sending proprietary documents and information out of the FDA. Some documents are may have the letter "K" followed by a string of six (6) numbers. Check to see if SUBJECT is sending these outside the FDA. Probably using Gmail to send out.

SUBJECT sent proprietary documents to press, possibly NY Times (Gartner Harris - sp?) - (Gardiner Harris - Corrected) for article alledging the FDA was mis-handling the Colonography topic.

His superiors believe HE is "ghost writing" his subordinates FDA reports. Check all possible avenues for possible occurances.

SUBJECT'S subordinates or co-horts:

[REDACTED]	DRL0091494
Paul T. Hardy	DRL0102315
[REDACTED]	DRL0101046 DRL5125449
Cindy Demian	DRL0101600
Nancy Wersto	DRL5114924
Lakshmi Vishnuvajjala	DRL5125617 DRL0096322

Check all for possible POP3 or enternal, non-FDA email conversations, either via Websense, Encase, Mandiant, or Spector.

**Spector Client: installed and active since 4/22/10**

**SUBJECT: Robert C. Smith (RCS)  
Medical Officer**

Hoofnagle testified that he received no legal guidance whatsoever from the FDA:

<sup>83</sup> Hoofnagle Tr. at 11-12.

<sup>84</sup> *Id.* at 12.

<sup>85</sup> Joseph Hoofnagle, Chickasaw Nation Industries Information Technology, *Spector Client: Installed and Active Since 4/22/10*. [hereinafter *Spector Client*].

Q. Over the course of [the monitoring], were you ever given any legal guidance about the limitations of surveillance or any legal considerations that would be relevant to using monitoring software?

A. No.

Q. At FDA, was there ever any guidance?

A. The only guidance I ever received was from law enforcement.

Q. Uh huh.

A. And it wasn't from a legal perspective. It was just from an authority perspective of, you know, hi, I need you to do this.<sup>86</sup>

In fact, CDRH leadership lacked sufficient training and background in conducting an internal investigation – particularly in monitoring computers. The contractors hired to conduct the computer monitoring received no legal guidance about the limitations of the monitoring—such as carving out communications with Congress or preserving protected attorney-client communications.<sup>87</sup>

After monitoring two employees' computers, contractors with CNIIT prepared an interim report to describe the status of the surveillance.<sup>88</sup> In the report, CNIIT contractors explained that they initiated a review of Dr. Smith's computer to determine whether he contacted external sources regarding the FDA's approval process of certain medical devices.<sup>89</sup>

---

<sup>86</sup> Hoofnagle Tr. at 25-26.

<sup>87</sup> See, e.g. Interim Report, *supra* note 10.

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

## Interim Report of Investigation

To: Lori Davis, Chief Information Officer  
CC: Joe Albaugh, Chief Information Security Officer  
From: Joe Hoofnagle, Incident Response and Forensic Lead; Christopher Newsom, Incident Response and Forensic Investigator  
Date: June 3, 2010  
Subject: Interim Report of Investigations - Robert C. SMITH

**“The Security Department has initiated a review of FDA data sources associated with SMITH to determine the validity of the allegations.”**

The Security Department has initiated a review of FDA data sources associated with SMITH to determine the validity of the allegations. The analytical findings to date appear to support the allegations, however the review is ongoing and substantial volumes of data are currently being culled.

The subordinate information that follows contains:

**“The subordinate information that follows contains . . . information indicating potential involvement of Congress member(s) . . . .”**

- FDA personnel that appear to be involved with the allegations,
- Communications with external press sources, including Gardiner Harris, reporter for the New York Times,
- Collaboration amongst FDA personnel and external sources to provide defamatory information about the FDA approval process as well as issues regarding hostile work environment and discrimination,
- Distribution of potentially sensitive information to external, non FDA sources, and
- Information indicating potential involvement of Congress member(s) serving as conduits to the press.

When asked about the interim report, Hoofnagle explained that the FDA officials who ordered the monitoring never voiced concerns that the information being captured was too extensive.<sup>90</sup> He testified:

- Q. So the very last bullet on the first page, it says, “information indicating potential involvement of Congress Member(s) serving as conduits to the press.” At that point, did anybody raise a concern that information like that should not be gathered or should not be reported up to Ruth McKee?
- A. No.
- Q. Did you ever hear that concern?
- A. No.

<sup>90</sup> Hoofnagle Tr. at 36-37.

Q. Did anyone from Ruth's office ever express to you any limitations or concerns about what was being collected?

A. No.

Q. Had you ever, in your experience, you know, with monitoring initiated by the inspector general's office, heard the concern that information about communications with Congress should not be collected or should not be communicated up the chain at FDA?

A. No.

Q. How about communications with the people under surveillance and their – between them and their personal attorneys?

A. No.

Q. Between them and the Office of Special Counsel?

A. No.

Q. In any of the surveillance, were limitations or concerns expressed about the scope of monitoring?

A. No.

Q. Nobody's ever come to you and said, we should maybe limit the scope of surveillance?

A. No.<sup>91</sup>

Dr. Jeffrey Shuren, the highest-ranking FDA employee involved in the monitoring, was equally unaware that the monitoring had captured communications with Congress.<sup>92</sup> He testified:

Q. Can you explain to us why you didn't take any steps to instruct Ruth McKee to do any kind of narrowing with regard to the scope of the monitoring – once you learned that Congressional communications were being captured?

A. I mean, as I said before, it wasn't even on my radar screen. And I don't recall when I first –

Q. When it came up?

---

<sup>91</sup> *Id.*

<sup>92</sup> Shuren Tr. at 123.

A. I don't recall when it first came up. But, no, it just – it didn't – it just didn't dawn on me. Didn't dawn on me.<sup>93</sup>

The Committees found that there was no documentation or written authorization for monitoring employees' computers, and the FDA personnel interviewed were uncertain as to who authorized surveillance.

The computer monitoring also did not include a retrospective inquiry into any of the scientists' network activities to understand who may have accessed the memoranda that were leaked to the press. The FDA managers and IT professionals interviewed failed to explain clearly how the rationale offered to justify the monitoring was consistent with the method used. There appeared to be confusion about the distinction between retrospective identification of individuals who already accessed certain documentation that was featured in the *New York Times* articles and real-time monitoring going forward once the internal inquiry began. Lori Davis testified that “at that first meeting I would have said [the search for evidence of leaks on FDA computers] was historical because...in my mind it had already happened.”<sup>94</sup>

Dr. Shuren described his concerns about both past leaks and the potential for future leaks.<sup>95</sup> He testified:

Q. Maybe it would be helpful for us if you clarified what exactly the purpose of the monitoring was. What was the question that you were trying to answer through the monitoring?

A. Well, again, what I...I didn't ask for monitoring. I didn't object to monitoring, but I didn't ask for monitoring. I had asked can we identify, are there ways to identify who was the source of the New York Times and the GE CT colonography device . . .

Q. So you wanted to try to figure out retrospectively who had made that leak as opposed to going forward if there were future leaks, can we kind of catch them as they occur?

A. Well, we all had concerns about future leaks. Once they were doing monitoring there was interest, are there other leaks that are occurring, but when I asked Ruth to look into what ways were available options, it was about finding the source of that.<sup>96</sup>

Ruth McKee, who acted as a liaison between Dr. Shuren and CNIIT, testified that “[her] understanding was there was not a technological way to do a past look” based on what she was told by the FDA Chief Information Officer, Lori Davis, and the FDA Chief Information Security

---

<sup>93</sup> *Id.*

<sup>94</sup> Davis Tr. at 8-11.

<sup>95</sup> Shuren Tr. at 32-33.

<sup>96</sup> *Id.*

Officer, Joe Albaugh.<sup>97</sup> Furthermore, McKee stated that it was her understanding that CNIIT “would be doing real time monitoring of Dr. Smith’s e-mail account.”<sup>98</sup>

Contrary to McKee’s testimony, however, Christopher Newsom, CNIIT investigator, testified that although his firm had the capability to look back at e-mails that may have been sent or received in the past through FDA servers, CNIIT did not conduct such a review.<sup>99</sup> Newsom testified:

Q. Is there a way to look, other than looking on the hard drive, to look for e-mails. . . in the past through FDA servers?

A. Yes.

Q. Was that done with regard to Dr. Smith or Dr. Nicholas?

A. Not to my knowledge.

Q. Do you know why not?

A. I don't.<sup>100</sup>

Not only was there insufficient written guidance on how to monitor an employee in compliance with applicable laws, it seems there was also inadequate knowledge or guidance on how to conduct the monitoring in order to accomplish the goals of initiating the monitoring in the first place. As Dr. Shuren testified, the goal was not only to capture future leaks, but to find the past leaks linked to the *New York Times*.<sup>101</sup> Yet, no one conducted an inquiry into past communications.

---

## VIII. Details of the Computer Monitoring

---

<b>FINDING:</b>	The goal of monitoring was allegedly to identify who leaked confidential information. Instead of looking back at previous communications, however, the FDA chose real-time monitoring of current and future communications. Because FDA managers lacked formal investigative training and did not understand the legal concerns related to employee monitoring, they believed all employee communications that occurred on government computers were “fair game.”
-----------------	---

---

<sup>97</sup> McKee Tr. at 58-60.

<sup>98</sup> *Id.*

<sup>99</sup> Newsom Tr. at 34-35.

<sup>100</sup> *Id.*

<sup>101</sup> Shuren Tr. at 19-20.

On April 22, 2010, the FDA began monitoring the FDA-issued computer and FDA-issued laptop of Dr. Robert Smith.<sup>102</sup> On May 24, 2010, the FDA began monitoring the FDA-issued computer of CDRH scientist Paul Hardy.<sup>103</sup> On June 30, 2010, the FDA began monitoring the FDA-issued computers of three additional CDRH scientists.<sup>104</sup>

To monitor these computers, the FDA used a computer monitoring software program called Spector 360, which allowed the FDA to record all computer activity in real-time. Spector 360 also has the ability to log keystrokes, capture passwords and confidential information, and record activity remotely in the event that a laptop being monitored is not directly connected to the FDA network.<sup>105</sup>

As part of the monitoring, the FDA took screen shots of each of the computers every five seconds and logged all keystrokes on the keyboards.<sup>106</sup> CDRH officials reviewed the information gathered through the monitoring using encrypted flash drives.<sup>107</sup> Information on the encrypted flash drives included private, non-official communications, including Gmail and Yahoo! Mail messages.<sup>108</sup> Transmitted information also contained communications with Congress, confidential attorney-client communications, and confidential complaints filed with the OIG and OSC.<sup>109</sup>

Spector 360 user activity monitoring software is readily available for both home and business use. The software “monitors, captures, and analyzes ALL user and user group activity including: e-mail sent and received, chat/IM/BBM, websites visited, applications/programs accessed, web searches, phone calls, file transfers, and data printed or saved to removal devices.”<sup>110</sup> FDA employees received no notice that this specialized software with such extensive monitoring capability was being installed on their computers.<sup>111</sup> Moreover, the FDA did not routinely subject all of its employees to such intense scrutiny.<sup>112</sup> CNIIT investigator Joseph Hoofnagle, installed the software, and his colleague Christopher Newsom collected the data.<sup>113</sup> The Spector 360 software does not distinguish or filter out any information, such as protected communications with Congress, communications covered by attorney-client privilege, or communications that might otherwise be protected by law, such as confidential submissions to the Office of Special Counsel. Moreover, those collecting and forwarding the information did not have any training or instruction in minimizing the collection of privileged communications.<sup>114</sup>

---

<sup>102</sup> *Spector Client*, *supra* note 85; Ireland Letter, *supra* note 6.

<sup>103</sup> *See* Ireland Letter, *supra* note 6.

<sup>104</sup> *Id.*

<sup>105</sup> Newsom Tr. at 10-11.

<sup>106</sup> *Id.*

<sup>107</sup> McKee Tr. at 13.

<sup>108</sup> *See e.g.*, Newsom Tr. at 54-55.

<sup>109</sup> McKee Tr. at 76.

<sup>110</sup> SpectorSoft Spector 360, <http://www.spector360.com> (last visited Feb. 21, 2014).

<sup>111</sup> McKee Tr. at 73.

<sup>112</sup> *Id.* at 83.

<sup>113</sup> Newsom Tr. at 8-10.

<sup>114</sup> *See e.g.*, Hoofnagle Tr. at 27-28.

The CNIIT contractors collected this information and summarized it for FDA managers' later review.<sup>115</sup>

Ancillary Actors

10. Ned Feder – Staff Scientist / Writer – POGO (Project On Government Oversight)  
1100 G Street, NW, Suite [REDACTED], Washington, D.C
11. [REDACTED] – Associate of Ned Feder  
Nuclear Engineering, Texas A&M University
12. Jack Mitchell - United States Senate, Special Committee on Aging  
G31 Dirksen or 628 Hart Senate Office Buildings, Washington, D.C.
13. Joan Kleinman – District Director, Congressman Chris Van Hollen (D-Md)  
Office of Representative, 51 Monroe Street #507, Rockville, Md.
14. Congressman Chris Van Hollen (D-Md)  
House of Representatives  
1707 Longworth H.O.B., Washington, D.C.  
District Office - 51 Monroe Street #507, Rockville, Md.

When asked whether they thought it was appropriate to gather attorney-client privileged communications, Hoofnagle responded:

- Q. Okay. So if you got that permission and you put Spector on, and you noticed someone communicating with their personal attorney, what
- A. I have not received instruction on that.
- Q. Okay. You don't know what you would do.
- A. You know, what I would do, I might say something. Because we're in an environment where, you know, obviously this is a problem. And I might say something. But, yeah, that process is evolving.
- Q. But you don't currently have a procedure that would allow . . . you to not capture those types of communications?

<sup>115</sup> Chickasaw Nation Industries Info. Technologies, Actors List (May 5, 2010). [FDA 1023-1024]

A. To not capture those types of communications is correct.<sup>116</sup>

In order to keep the information secure, CNIIT used two encrypted flash drives to deliver information to FDA officials for review. When the CNIIT investigators found information they believed to require further review, they would flag this information when they forwarded it to FDA officials. Specifically Ruth McKee, served as the “contact point between [Office of Information Management] and the center [CDRH].”<sup>117</sup> McKee testified that although she had access to all the information, the information she passed on to her superiors did not contain the communications with Congress or any other protected communications.

Q. [D]id you or Mary Pastel provide summaries of the information that was being captured to either people above you in the chain of command or to the employees' supervisors?

A. Only relevant to disclosure of information, agency information.

Q. Right. To Members of Congress, to OSC?

A. No. No. Only relevant information.

Q. Why not?

A. Why not what?

Q. Well, your goal I thought was to look at disclosures to outside parties, right?

A. Right.

Q. **And nobody ever told you that it was inappropriate to look at disclosures to OSC or Members of Congress or attorneys, right?**

A. **Right.**

Q. **And you thought that was fair game because they were doing it on an FDA computer, right?**

A. **I thought monitoring was fair game.**<sup>118</sup>

---

<sup>116</sup> Hoofnagle Tr. at 39.

<sup>117</sup> McKee Tr. at 57.

<sup>118</sup> *Id.* at 76-77 (emphasis added).

---

## IX. Evolution of the Monitoring Program

---

**FINDING:** The monitoring program began when a law firm representing a manufacturer alleged unlawful disclosures were made to the press regarding a device that was under FDA review. Ruth McKee first ordered the monitoring on Dr. Smith's computer because Dr. Smith was believed to be the source of the leak. Later, monitoring expanded to include four additional CDRH scientists. Officials used Spector 360, a software package that recorded user activity with powerful capture and analysis functions, including real-time surveillance.

**FINDING:** The FDA's surveillance was not lawful, to the extent that it monitored communications with Congress and the Office of Special Counsel. Federal law protects disclosures to OSC and Congress.

### ***B. Initiation of Monitoring***

FDA officials conducted surveillance of employees' computer information in response to an April 16, 2010, letter from GE Healthcare's outside counsel.<sup>119</sup> GE Healthcare alleged the disclosure of confidential information to the press regarding the company's premarket notification submission for a CT scanning device for colonography screening.<sup>120</sup> Ruth McKee, CDRH's Executive Officer, led the agency's effort to determine what it could do in response to the allegations contained in the letter, which, ultimately, was to initiate the monitoring of CDRH employees' computer activity. McKee testified:

Q. How did it fall to you in this case to initiate the investigation?

A. I think giving me credit for initiating an investigation is giving me more credit than I am due. I was the executive officer for the organization where the allegation arose. It was my job to try to figure out what options we had.<sup>121</sup>

The FDA's computer monitoring program appears to have been unprecedented in scope and intensity. In the past, monitoring activities were limited to activities like high-bandwidth transfers of data or viewing pornography on government computers.<sup>122</sup> McKee instructed Mary Pastel, Deputy Director for Radiological Health in the CDRH's Office of *In Vitro* Diagnostics and Radiological Health, to review surveillance materials collected on the encrypted flash drives. This was the first time she had received instructions to review such close surveillance of

---

<sup>119</sup> Basile Letter, *supra* note 58.

<sup>120</sup> *Id.* at 2.

<sup>121</sup> McKee Tr. at 29-30.

<sup>122</sup> Davis Tr. at 34.

employees' computer activity. McKee did not provide any monitoring boundaries or limitations. Pastel testified:

Q. Okay. Had you ever been asked to do a project like that before?

A. A project like what?

Q. Like reviewing - from a computer that was under surveillance.

A. No.

Q. Did anybody give you any guidance about how to do that besides the instructions that Ruth gave you?

A. No.<sup>123</sup>

Initially, the FDA monitored only one employee, Dr. Robert Smith. In April 2010, Lori Davis approached Joe Albaugh, who was then the FDA's Chief Information Security Officer, to set up monitoring for Dr. Smith.<sup>124</sup> The FDA set up monitoring of Dr. Smith on April 22, 2010, five days after FDA's receipt of the GE letter. Albaugh testified:

Q. Can you describe for us what Lori told you?

A. That . . . the executive officer had approached her and that the concern was about confidential information that had been leaked to the public.

Q. And what did Lori ask you to do?

A. To work with the . . . executive officer at CDRH, to set up monitoring . . . for an individual who they believed to be responsible for the leakage.

Q. When you say "executive officer," can you tell us that person's name?

A. That was Ruth McKee.<sup>125</sup>

When Davis ordered the surveillance, she offered no guidance, alternative approaches, or instructions on how to conduct the monitoring.<sup>126</sup> Along with the FDA officials' failure to give any instructions about appropriate protocol for the monitoring, officials also failed to offer

---

<sup>123</sup> H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Mary Pastel, at 23 (Jan. 4, 2013) [hereinafter Pastel Tr.].

<sup>124</sup> Albaugh Tr. at 6-8.

<sup>125</sup> *Id.* at 6-7.

<sup>126</sup> *Id.* at 9-10.

guidance about possible legal implications of a broad-based surveillance of private information such as communications with attorneys or Congress. Pastel testified:

Q. Did anybody talk about the legal guidelines or other things that might be worth paying attention to, such as the reason that we're kind of here today is because communications with Congress, with OSC, with some of these people's personal attorneys were captured and reviewed. And Chairman Issa and Senator Grassley were concerned about that, especially since some of Senator Grassley's staff were folks, you know, whose communications were being captured.

So my question is, did anybody ever suggest to you, you know, let's exclude those communications from the scope of this review? If you see anything like that, you know, don't forward them along to whoever you were handing the material back to? Did you ever get guidance along those lines?

A. **No. These were communications on government computers. And we have government computer security training every year, and in that security training it says that anything on the government computer can get monitored.**<sup>127</sup>

### ***C. Type of Monitoring***

Some FDA officials stated they did not fully appreciate the scope of the surveillance or the intrusiveness of the Spector 360 user activity monitoring software installed on employees' computers. While at least one FDA official was under the impression that *only* a retrospective search would be conducted to attempt to determine if an employee had leaked information to the press, another official was well aware that real-time surveillance would be the protocol used by the CNIIT investigators.

Executive Officer Ruth McKee stated:

Q. Okay. So then what is it that you thought that IT was going to be doing in response to your request about that topic?

A. I didn't know what they were going to be doing. That's why I went to talk to them.

Q. Right. And after the discussion, what was your understanding of what they would be doing?

---

<sup>127</sup> Pastel Tr. at 23-24 (emphasis added).

A. That they would be doing real-time monitoring of Dr. Smith's email account.

Q. For future communications?

A. Yes.<sup>128</sup>

On the other hand, CIO Lori Davis maintained that she was unaware that the monitoring would include real-time surveillance. Davis stated:

Q. So, at this first meeting, did you contemplate that this would be a historical search, a search of existing e-mails in the past to determine who had been responsible for this particular leak? Or were you anticipating that there would be real-time monitoring going forward?

A. At that first meeting, I would have said it was historical . . . because in my mind, it had already happened.<sup>129</sup>

\* \* \*

Q. Uh huh. So when did you understand?

A. I am going to tell you that I don't think I ever knew that they were doing real-time monitoring to the extent that it was reported on.

Q. You mean in the press?

A. In the press.

Q. So when you read the press reports about screen shots every 6 seconds

A. That's the first that I have learned the extent of what that real-time monitoring looked like.<sup>130</sup>

#### ***D. Development of Search Terms***

Ruth McKee was responsible for determining the initial search terms for the employee computer monitoring project. The FDA's Office of Information Management (OIM) used these search terms to provide summaries and examples of the captured information to management.<sup>131</sup>

---

<sup>128</sup> McKee Tr. at 59.

<sup>129</sup> Davis Tr., at 11.

<sup>130</sup> *Id.* at 24.

<sup>131</sup> McKee Tr. at 9.

Even after the surveillance began, McKee never asked for or received any feedback from OIM about limiting or expanding the scope of the surveillance. McKee testified:

Q. Okay. Did you ever get any feedback from Dr. Shuren or anybody else about what was being collected?

A. Describe "feedback."

Q. Did they give you any guidance to either limit or expand the scope of the surveillance? Did they suggest additional search terms, or did they say, keep doing what you are doing, this seems to be working?

A. **No additional guidance, no. Not to expand search terms or to make changes, no.**<sup>132</sup>

### ***E. Interim Report***

Christopher Newsom and Joseph Hoofnagle, CNIIT investigators, drafted an interim report to summarize the status of the surveillance.<sup>133</sup> Prior to finalizing the interim report, CNIIT investigators met with FDA managers to review the document.<sup>134</sup> Little, if any, planning, however, went into the preparation of the report. Hoofnagle and Newsom did not receive any guidance on what to include. McKee testified:

Q. In the interim report, when you met to discuss this document, did anybody have any concerns about the language that was used in here?

A. No.

Q. Was the language used in here – did Chris or Joe receive any guidance on how they should create this document? Were they given a framework by which to present the evidence that they uncovered?

A. Not that I am aware of, no.

Q. This is something they devised themselves, as far as you know?

A. That is my understanding.<sup>135</sup>

---

<sup>132</sup> *Id.* at 22 (emphasis added).

<sup>133</sup> Hoofnagle Tr. at 34.

<sup>134</sup> McKee Tr. at 26-27.

<sup>135</sup> *Id.* at 91-92.

Newsom explained that no one at the FDA gave him any guidance on writing the report. He testified:

Q. Did anybody give you any guidance on the language in the interim report?

A. No.

Q. That was all your own?

A. Yes.<sup>136</sup>

On June 3, 2010, CNIIT sent the report to Davis and Albaugh.<sup>137</sup> McKee viewed the report soon after.<sup>138</sup> The report summarized the surveillance conducted thus far of Dr. Smith's official and personal e-mail accounts, including e-mails with journalists, congressional staff members, and the Project on Government Oversight.<sup>139</sup>

- Multiple Gmail contacts with Jack Mitchell (aging.senate.gov) – Emails include attachments with significant amount of documents including those self-redacted.

View All instances of the above noted in order by date

- Multiple Gmail contacts with Joan Kleinman (District Director for Rep. Chris Van Hollen) – Emails include attachments with significant amount of documents including those self-redacted.

View All instances of the above noted in order by date

The interim report also alleged that Dr. Smith “ghostwrote” his subordinates’ reports and supplied internal documents and information to external sources.<sup>140</sup> The report confirmed that Dr. Smith spoke with colleagues who shared his concerns about the approval of potentially dangerous products.<sup>141</sup> These colleagues also worked with Dr. Smith to shed light on these alleged improprieties.<sup>142</sup> Prior to the issuance of the interim report, the FDA began monitoring CDRH scientist Paul Hardy’s computer. Following the report, FDA officials expanded the surveillance to more CDRH employees.

---

<sup>136</sup> Newsom Tr. at 122.

<sup>137</sup> Interim Report, *supra* note 10.

<sup>138</sup> McKee Tr. at 26.

<sup>139</sup> Interim Report, *supra* note 10.

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

<sup>142</sup> *Id.*

## ***F. Expansion of People Monitored***

Soon after writing the interim report, monitoring was expanded to three additional CDRH employees.<sup>143</sup> McKee explained her role in permitting the monitoring of additional employees, acknowledging she initiated and expanded the surveillance with the approval of Dr. Shuren and others. She stated:

- Q. Okay. What was your – describe your role to me, as you understand it.
- A. I was essentially – I was the contact point between LIM and the center.
- Q. When you say you were the contact point, you initiated the scope of monitoring. Correct?
- A. Yes.
- Q. And it was your decision to expand the scope of the monitoring to the additional FDA employees, correct?
- A. Not only my decision, no.
- Q. Right. You had to seek Dr. Shuren’s approval of that?
- A. And there were discussions held, I believe, above Dr. Shuren’s level.<sup>144</sup>

Christopher Newsom testified that fellow CNIIT investigator Joseph Hoofnagle, along with Joe Albaugh from the FDA, instructed him to expand the surveillance.<sup>145</sup>

## ***G. Changes to the FDA Employee Login Disclaimer***

Every employee within the FDA receives a brief login disclaimer before logging into a government computer explaining that their activities on the computer could be monitored. The FDA, however, changed the message on the disclaimer before the monitoring program began.<sup>146</sup> Initially, the disclaimer stated that for the purpose of protecting the FDA’s property, information accessed on the computer could be “intercepted, recorded, read, copied, or captured in any manner and disclosed by and to authorized personnel.”<sup>147</sup>

---

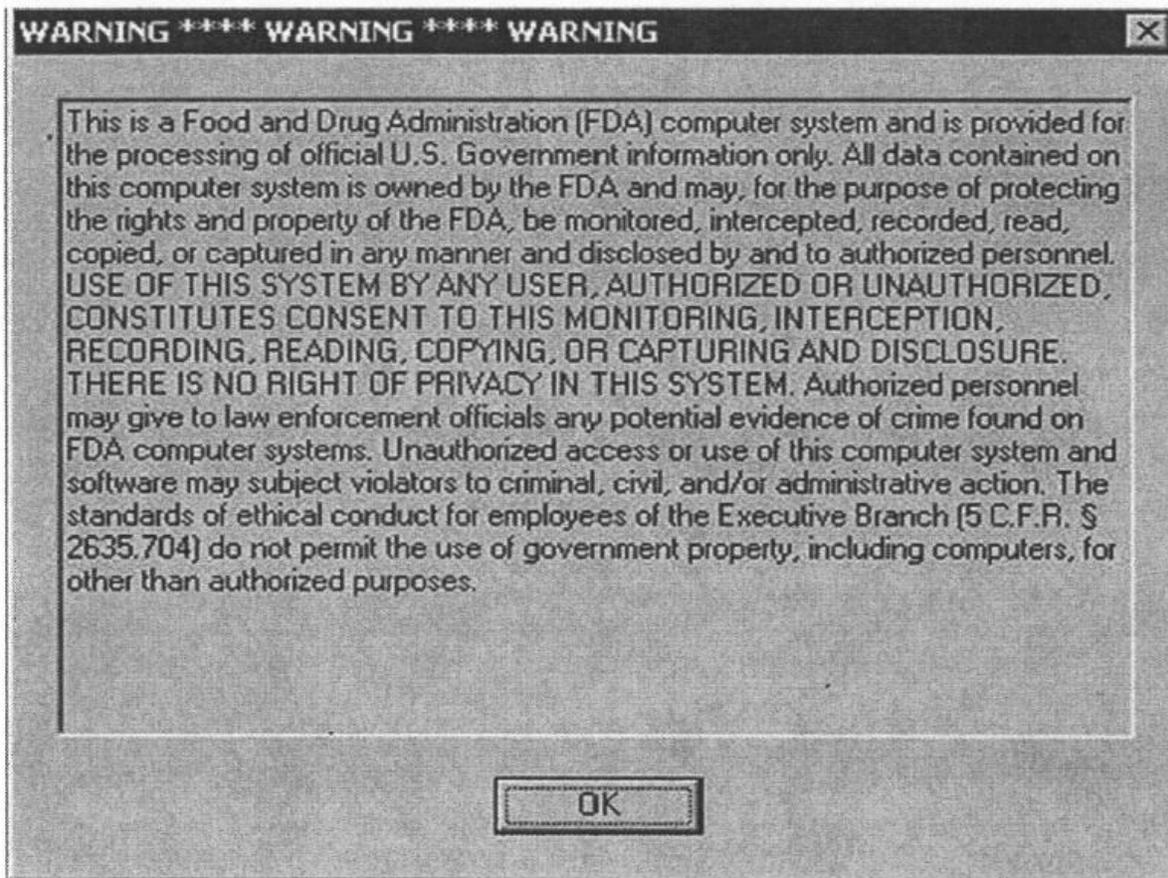
<sup>143</sup> McKee Tr. at 16.

<sup>144</sup> *Id.* at 57-58.

<sup>145</sup> Newsom Tr. at 122.

<sup>146</sup> Davis Tr. at 54.

<sup>147</sup> *Id.* at 53, Exhibit 7, FDA Employee Login Disclaimer.



In her testimony, Lori Davis, the FDA Chief Information Officer, described the purpose of the warning message.<sup>148</sup> She also explained that Joe Albaugh, the FDA Chief Information Security Officer, had the capacity to change the disclaimer language.<sup>149</sup> Davis testified:

- Q. This is the FDA warning banner. Do you recall – well, first describe to us what this is.
- A. This pops up when you power on your machine. It's probably one of the first things all employees see when they log onto their FDA computer.
- Q. And who is responsible for coming up with this text and/or making any edits or changes to the text if need be?
- A. Joe Albaugh worked – and I don't recall whether or not it was the Office of Inspector General that he worked with it or Office of Legal Counsel at HHS. But he worked either with OIG or Office

---

<sup>148</sup> *Id.* at 53-54.

<sup>149</sup> *Id.*

of Chief Counsel – you have to ask him – on editing this language.<sup>150</sup>

Davis later explained that Albaugh changed the disclaimer language because he did not believe the prior language was “tight enough.”<sup>151</sup> Although no other FDA Officials interviewed could recall when the change was made, Davis stated that Albaugh decided, to edit the message before monitoring began on CDRH scientists and doctors.<sup>152</sup> Davis stated:

Q. So you recall a change in this language –

A. Correct.

Q. -- at some point while you were there?

A. Correct.

Q. Okay. Can you tell me what precipitated the change and why?

A. You’ll have to ask – **in Joe’s mind, he felt that the language was not tight enough.**

Q. When did he – he expressed that concern to you at some point?

A. Yes.

\* \* \*

Q. Do you recall whether it was after the monitoring in this case had already begun?

A. No, it was before.<sup>153</sup>

Mr. Albaugh, however, could not recall any specific changes made or when they occurred, only that he was sure changes were made.<sup>154</sup>

According to documents obtained by the Committee, the disclaimer message was edited to explain to users that they have no reasonable expectation of privacy when using the FDA security system.<sup>155</sup> The prior disclaimer was significantly expanded to list specific devices which encompassed the U.S. Government information system, and outlined additional details about what information the FDA could monitor on the computer.<sup>156</sup> These personal storage

---

<sup>150</sup> *Id.*

<sup>151</sup> Davis Tr. at 54.

<sup>152</sup> *Id.*

<sup>153</sup> *Id.* (emphasis added).

<sup>154</sup> Albaugh Tr. at 34.

<sup>155</sup> See Ireland Letter, *supra* note 6.

<sup>156</sup> *Id.*

devices were ultimately monitored and searched in the FDA monitoring investigation. The revised disclaimer stated:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information, you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.<sup>157</sup>

Regardless of when the banner was changed to address, among other things, personal storage devices that were attached to agency computers, it did not discuss the intrusive search procedures to which those personal storage devices attached to the FDA network would be subject.

In the course of the FDA monitoring investigation, CNIIT investigator Chris Newsom used Encase, a forensic imaging tool used to recover specific documents, including deleted files, artifacts, and information from unallocated space, to retrieve data from the personal storage device of one of the five employees being monitored.<sup>158</sup> Therefore, the employees being monitored were not only subject to real-time monitoring of activity on FDA computers, but also to an additional layer of intrusion involving personal storage devices. Encase was used to reconstruct and copy personal files that FDA employees had deleted from their personal storage device before plugging that device into an FDA computer. That level of surveillance is not reasonably contemplated by the phrase in the FDA's disclaimer, which merely asserts that a "government information system" includes "all devices and storage media attached to this network."

---

<sup>157</sup> *Id.*

<sup>158</sup> Newsom Tr. at 27, 63.

---

## X. The Office of Inspector General Declines to Investigate

---

**FINDING:** HHS OIG denied FDA’s repeated requests for an OIG investigation into the allegedly wrongful disclosures. OIG found no evidence of criminal conduct on the part of any employee. Still, officials continued to contact OIG to request an investigation. OIG again denied the request, and the Justice Department declined to take action.

When Dr. Shuren learned about the extent of the confidential disclosures of Dr. Smith and other employees, he wrote to the FDA Office of Internal Affairs (IA), which in turn referred the matter to the Office of Inspector General.<sup>159</sup> Les Weinstein, the Ombudsman for the CDRH, contacted the OIG to request an investigation into Dr. Smith’s disclosure of confidential information to the press.<sup>160</sup> Dr. Shuren was copied on the e-mail request to the OIG.<sup>161</sup> On May 14, 2010, IA wrote to the OIG in response to the allegations contained in GE Healthcare’s April 16, 2010, letter.<sup>162</sup> In its response, IA asked the OIG to investigate any disclosure of confidential information by CDRH employees.<sup>163</sup>

In response, the OIG wrote to IA on May 18, 2010, stating the wrongful disclosure allegations “lack any evidence of criminal conduct on the part of any HHS employee.”<sup>164</sup> The OIG added that federal law permits disclosures to the media and Congress when related to matters of public safety, so long as the information is not protected by national security interests or any other specific prohibitions.<sup>165</sup> Later, the OIG clarified the statement to mean that the OIG did not have the authority to determine the legality of such disclosures.<sup>166</sup> Instead, the OIG could refer matters to the Department of Justice if there were “reasonable grounds to believe” there was a criminal law violation.<sup>167</sup> The OIG clarified that the final determination on whether there is potential criminality was the Justice Department’s responsibility.<sup>168</sup>

On June 28, 2010, Dr. Shuren again wrote to the OIG with a new request for an investigation.<sup>169</sup> He explained that the FDA had acquired new information regarding the disclosures based on an internal investigation.<sup>170</sup> He reiterated that the disclosures, which were prohibited by law, had continued for quite some time.<sup>171</sup> His letter explained that FDA officials

---

<sup>159</sup> Shuren Tr. at 14.

<sup>160</sup> Weinstein E-mail, *supra* note 16.

<sup>161</sup> *Id.*

<sup>162</sup> Letter from Mark S. McCormack, Special Agent in Charge, Office of Internal Affairs, FDA, to Scott A Vantrease, Office of Inspector Gen., HHS (May 14, 2010).

<sup>163</sup> *Id.*

<sup>164</sup> Vantrease Letter, *supra* note 17.

<sup>165</sup> *Id.*

<sup>166</sup> Letter from Elton Malone, Office of the Inspector Gen., HHS, to Mark McCormack, Office of Internal Affairs, FDA (Jul. 26, 2012).

<sup>167</sup> *Id.*

<sup>168</sup> *Id.*

<sup>169</sup> Shuren Letter, June 28, 2010, *supra* note 19.

<sup>170</sup> *Id.*

<sup>171</sup> *Id.*

conducted their own investigation because they believed an employee had leaked confidential proprietary information.<sup>172</sup> Dr. Shuren noted that IA authorized OIM to conduct real-time monitoring of Dr. Smith's computer.<sup>173</sup> He enclosed excerpts of the investigative findings and asked the OIG to review the communications to determine whether employees engaged in unlawful conduct.<sup>174</sup>

On November 3, 2010, the Justice Department wrote to the HHS OIG.<sup>175</sup> The Justice Department explained that the Criminal Division would decline prosecution.<sup>176</sup> The OIG concurred with the Justice Department's decision not to prosecute because "the referral lack[ed] any evidence of criminal conduct on the part of any HHS employee."<sup>177</sup>

On February 23, 2011, Dr. Shuren wrote for the third time to the OIG to request an investigation into two FDA employees' nonconsensual recording of phone calls and meetings regarding FDA business.<sup>178</sup> He added that the nonconsensual recordings were potential violations of state and/or federal wiretapping laws, which, in some instances, require consent of the parties to the communication.<sup>179</sup> Dr. Shuren noted that violations of wiretapping laws are felonies, which may subject the person in question to fines and imprisonment.<sup>180</sup> He further explained that there was no FDA policy that permitted the unauthorized recording of phone calls and employee meetings, or the use of FDA equipment for surveillance.<sup>181</sup> Additionally, he expressed concerns over the storage of the recordings, noting the agency's requirements for secured storage and destruction of sensitive information.<sup>182</sup>

In March 2011, Ruth McKee also wrote to the OIG in reference to the alleged recordings. The OIG responded to Ruth McKee on June 10, 2011, and declined to investigate the matter.<sup>183</sup> Rather, the OIG deferred to the FDA for any necessary administrative action.<sup>184</sup> Still, the monitoring continued according to Dr. Shuren.<sup>185</sup>

Q. I'm trying to understand the distinction between continuing to pursue the investigative track, by which I mean monitoring, and then the administrative track, which sounds like it started shortly after you got that letter. But simultaneously the surveillance continued. Is that correct?

---

<sup>172</sup> *Id.*

<sup>173</sup> *Id.*

<sup>174</sup> *Id.*

<sup>175</sup> DOJ Letter, *supra* note 21.

<sup>176</sup> *Id.*

<sup>177</sup> Vantrease Letter, *supra* note 17; E-mail from Kenneth Marty, Special Investigations Branch, Office of Inspector Gen., Dep't of Health & Human Servs. to Ruth McKee, Exec. Officer, Ctr. for Devices & Radiological Health, FDA (June 10, 2011, 1:37 p.m.) [hereinafter Inspector Gen. E-Mail].

<sup>178</sup> Shuren Letter, Feb. 23, 2011, *supra* note 16.

<sup>179</sup> *Id.* at 2.

<sup>180</sup> *Id.*

<sup>181</sup> *Id.*

<sup>182</sup> *Id.* at 1-2.

<sup>183</sup> Inspector Gen. E-mail, *supra* note 177.

<sup>184</sup> *Id.*

<sup>185</sup> Shuren Tr. at 41.

A. Yes.<sup>186</sup>

When asked about the multiple requests for an OIG investigation into the disclosures, McKee expressed disappointment at the OIG's decision not to investigate. She stated:

Q. Okay. At a number of points along the way facts, evidence was referred to the Inspector General's Office. There were a series of letters asking the IG to take up this matter. Were you surprised or disappointed or did you have any reaction when the Inspector General's Office declined?

A. Yes.

Q. Can you describe for us what that reaction was?

A. Surprised and disappointed.

\* \* \*

Q. Why then were a series of additional efforts made to refer this to the IG after it had been declined more than once?

A. The additional referrals were for different topics.

Q. Okay. So there was a hope that while the IG had set aside the communicating proprietary information outside the agency piece of the puzzle, that maybe they would take up the patent issue or the one party recording issues?

A. Yes.

Q. **And they declined at each step of the way?**

A. **Yes, they did.**<sup>187</sup>

---

## **XI. Monitoring Was Not the Solution**

---

<b>FINDING:</b>	The monitoring program failed to identify who leaked information to the <i>New York Times</i> or the <i>Wall Street Journal</i> , despite capturing approximately 80,000 documents.
-----------------	---

---

<sup>186</sup> *Id.*

<sup>187</sup> McKee Tr. at 90-91 (emphasis added).

The whole point of initiating the monitoring of the five FDA employees was to confirm the suspicions of FDA management that these employees were, in fact, leaking information to the press. At the direction of FDA officials, the monitoring program collected approximately 80,000 documents.<sup>188</sup> Interviews with key FDA officials made it clear that the program did not accomplish what it was set up to achieve. For example, Dr. Shuren stated:

Q. Okay. So you never actually found proof that Robert Smith was disclosing [information] it to the press?

A. Confidential information?

Q. Yes.

A. Not to my recollection.<sup>189</sup>

In fact, in an effort to be thorough, FDA officials even reviewed Dr. Robert Smith's FDA-issued computer once he left the agency following the expiration of his contract but found no evidence of disclosures of confidential information to the media.<sup>190</sup>

FDA management went to unprecedented lengths in order to determine who was leaking confidential information to the press. Yet, they failed to find proof of leaks to the press. In fact, the only information FDA officials uncovered on one of the five FDA scientists monitored, Paul Hardy, was information disclosed to Congress – a protected form of communication.<sup>191</sup>

---

## **XII. Managing By Investigation**

---

<b>FINDING:</b>	Despite known complaints about performance issues regarding Dr. Robert Smith, FDA management and leadership chose to address Dr. Smith's employment status through an investigation rather than by simply taking an administrative action.
-----------------	--

Over the course of the investigation, it became evident that FDA officials chose not to address Dr. Robert Smith's job performance through administrative procedures available to them. Instead, FDA officials used the HHS OIG and computer monitoring tactics to investigate him. Dr. Robert Smith, the first scientist FDA officials monitored, was a thorn in the agency's side. According to Dr. Shuren, Dr. Smith created a "toxic" environment. Dr. Shuren stated:

The work environment was toxic and had bled over to other parts of the center as well. And that was a – radiological devices was a hornet's nest.

---

<sup>188</sup> Newsom Tr. at 132.

<sup>189</sup> Shuren Tr. at 93.

<sup>190</sup> Newsom Tr. at 32.

<sup>191</sup> McKee Tr. at 17-18.

It was essentially two camps. It was the people who were – Robert and his supporters, and there [were] other people or people who just wanted to stay out of the way.

People felt intimidated to speak up. There were people who I spoke to regarding what was going on in the office and some of them, I asked if they would speak to other investigators and OIG and others. And they declined to do so. They didn't even want to talk about it.

We had reviews being held up. They were just not going anywhere. And there wasn't an issue about science. Some of these were tactics of a meeting was being scheduled, and they'd say, we're not meeting – an internal meeting – until you give us an agenda. Then we want to see all e-mails between managers and the company before we actually agree to come in for an internal meeting. I mean, there was one thing – there was one thing after the other.

Early on, one of the things Robert I think even put this in writing, his position was if a manager didn't have adequate experience or expertise, his perspective, and they disagreed with another scientist, that is retaliation. By its nature. I mean, those were the kind of things we were dealing with.

And it was – it was constant. It was one thing after another.<sup>192</sup>

When asked whether FDA officials attempted to resolve this “toxic” environment through administrative measures rather than investigative channels, Dr. Shuren responded that senior management had rejected earlier attempts to discontinue Dr. Smith's contract. He stated:

A. I mean, he had managers in different offices at different times talk to him about his bad conduct. He received a number of cautions as well.

Q. These are the specific questions I want to ask about.

A. . . . But we also had the management team, you have to remember. So for these managers who also want to do something, they had the Assistant Commissioner for management, they had the lawyers, the HHS lawyers from General Law Division, these are the employment lawyers, and you have labor and employee relations, and that is what that mechanism was, the managers actually were going to them about what do we do in the circumstances, and they were hearing back from those people, this is what you should be doing. It wasn't about ignoring Robert Smith at all, but they were

---

<sup>192</sup> Shuren Tr. at 43.

getting their advice on what to do, they were talking with Robert, there was memo of cautions.

\* \* \*

Q. **So my understanding is a letter of caution is not an adverse personnel action as a technical matter.**

A. **Right.**

\* \* \*

Q. So this group, this management group that you described, you participated in the discussions with them and with Robert Smith's managers about various steps to take?

A. No, I for the most part was not part of the managers team. I got pulled into some things a little bit more than I normally would simply because of the circumstances. **So even on the managers for Robert not wanting to renew his contract, they came to me because they were concerned about would the Office of Commissioner not let them, if you will, not renew his contract, essentially saying you have to renew it.** Two years before the managers did not want to renew Robert's contract, and the Office of Commissioner stepped in and told them you will have to renew it, **and they were worried, even though it is different people, they were worried about the same thing. So I told them, I will support you, and I went to the Commissioner's office about will they support not renewing the contract, and even that decision on not renewing the contract and the memo regarding it went all the way up to the Acting General Counsel at HHS for review.**<sup>193</sup>

So, according to Dr. Shuren, managers initially renewed Dr. Smith's contract even though there were significant concerns about his performance. Then, despite continued problems and a letter from the OIG deferring to the FDA to take administrative action, senior FDA officials chose to address Dr. Robert Smith's alleged shortcomings through repeated referrals to the OIG for criminal investigation, rather than through direct management action.

---

<sup>193</sup> *Id.* at 82 (emphasis added).

---

## XIII. Post-Monitoring Changes

---

**FINDING:** Over a year after receiving directives from OMB, OSC, and the FDA Commissioner, the FDA produced interim guidelines on monitoring procedures in September 2013. The FDA’s interim policies require written authorization prior to initiating employee monitoring. Only the Commissioner, Deputy Commissioner, or the Chief Operating Officer can authorize surveillance of employees. The FDA has not yet implemented permanent policies to govern employee monitoring.

**FINDING:** The FDA’s interim policies do not provide safeguards to protect whistleblowers from retaliation. Under these policies, protected communications are still subject to monitoring and may be viewed by agency officials.

In response to the intrusive nature of FDA’s computer monitoring, the federal government took the unprecedented step of acknowledging that excessive monitoring could violate the law. On June 20, 2012, the Office of Management and Budget (OMB) sent a memorandum urging all Executive Branch departments and agencies to review their employee monitoring policies.<sup>194</sup> The memorandum is the first acknowledgment by the federal government that there are limitations on surveillance of government employees’ computers.

In particular, the memorandum recognizes that the government may not conduct unlimited computer surveillance, even when an employee is on duty and operating a government-owned computer.<sup>195</sup> Further, the memorandum also purports to safeguard protected communications made using private e-mail accounts.<sup>196</sup> Specifically, OMB instructed agencies to “take appropriate steps to ensure that those policies and practices do not interfere with or chill employees’ use of appropriate channels to disclose wrongdoing.”<sup>197</sup> OMB enclosed a memorandum from OSC highlighting that federal law protects whistleblowers’ rights.<sup>198</sup>

According to OSC, while lawful agency monitoring of employee electronic communications may serve a legitimate purpose, agencies should ensure these policies and practices do not interfere with or deter employees from using appropriate channels to disclose wrongdoing.<sup>199</sup>

---

<sup>194</sup> Memorandum from Steven VanRoekel, OMB Fed. Chief Information Officer, & Boris Bershteyn, OMB General Counsel, *Office of Special Counsel Memorandum on Agency Monitoring Policies and Confidential Whistleblower Disclosures* (June 20, 2012).

<sup>195</sup> *See id.*

<sup>196</sup> *See id.*

<sup>197</sup> *Id.*

<sup>198</sup> *See id.*

<sup>199</sup> Lerner Memo, *supra* note 24.

OSC addressed the issue of electronic monitoring and protected communications with OSC and OIGs.<sup>200</sup> The memorandum failed, however, to acknowledge whistleblowers' rights to communicate with Congress.<sup>201</sup> OSC issued a press release on February 15, 2012, acknowledging that monitoring employee e-mails should not dissuade employees from making disclosures to Congress.<sup>202</sup> Unlike the OSC memorandum, however, the press release was not circulated government-wide and did not receive as much attention. As a result, agencies have not received official notice from OMB or OSC that computer monitoring guidelines should ensure that protected communications include communications with Congress. If the Executive Branch has a legitimate reason for excluding communications with Congress from those that should be protected, it has not explained what that reason might be.

On September 24, 2012—shortly after OSC released its memorandum—FDA Commissioner Margaret Hamburg directed Elizabeth Dickinson, the FDA Chief Counsel, to alert the agency that future installation of Spector 360 software would require “written approval by the FDA Chief Counsel or her delegee.”<sup>203</sup> Commissioner Hamburg also directed the CIO and Chief Counsel to “promptly” develop written standards and procedures for monitoring employee personal work computers.<sup>204</sup>

Despite the urgency expressed by the Commissioner, FDA did not release any additional guidelines until over a year later. On September 26, 2013, Chief Operating Officer (COO) and Acting Chief Information Officer (CIO) Walter Harris released interim guidelines outlining new procedures for employee monitoring.<sup>205</sup> The interim guidelines have not yet been fully implemented, and are subject to change as the FDA continues to develop policies that are consistent with HHS monitoring policies. The FDA Commissioner's September 2012 memorandum, therefore, still acts as the guiding document. The interim guidelines included the following:

- Basis for computer monitoring
- Express written authorization
- Establishment of a review committee
- Limitations on time, scope, and invasiveness
- Periodic review by the COO
- Legal review of monitoring requests by FDA Office of the Chief Counsel<sup>206</sup>

---

<sup>200</sup> *Id.*

<sup>201</sup> *Id.*

<sup>202</sup> U.S. Office of Special Counsel, Press Release, *Office of Special Counsel Opens Investigation into FDA's Surveillance of Employees' E-mail* (Feb. 15, 2012).

<sup>203</sup> Memorandum from Elizabeth Dickinson, FDA Chief Counsel, *Requirements for Deploying Spector Software* (Aug. 1, 2012).

<sup>204</sup> Memorandum from Margaret A. Hamburg, FDA Commissioner to Walter A. Harris, FDA Chief Operating Officer, Eric Perakslis, Chief Information Officer, & Elizabeth H. Dickinson, FDA Chief Counsel, *Monitoring of FDA Personnel Work Computers* (Sept. 24, 2012).

<sup>205</sup> FDA Information Resources Management – Information Technology Security, *Monitoring of Use of HHS/FDA IT Resources* (Sept. 26, 2013).

<sup>206</sup> *Id.*

Although FDA's interim policies propose to establish procedures for regulating employee monitoring, the policies do not provide protections against whistleblower retaliation. Even with national media attention, recommendations from outside agencies, and internal agency directives, FDA has yet to implement permanent policies and procedures. Additionally, as of the date of this report, multiple inquiries are still pending, including two OIG reviews requested by the Secretary of HHS.

---

## **XIV. Conclusion**

---

The FDA's secret monitoring of CDRH employees is a prime example of a flawed oversight process for employee computer surveillance. A federal agency may monitor employees' computers for a lawful purpose. Retaliatory motives and excessively intrusive monitoring schemes that capture legally protected communications, however, are inappropriate.

The lack of appropriate limitations and safeguards in conducting employee surveillance has long been a concern of the Committee on Oversight and Government Reform. In 2012, the Committee learned of a similarly flawed employee surveillance program at the Federal Maritime Commission (FMC). Like the FDA, the FMC used Spector 360 to conduct covert surveillance of a select group of employees. The FMC allegedly targeted for surveillance employees who expressed opinions which contradicted the Chairman's views. Furthermore, the FMC OIG requested that agency management stop using the monitoring software, citing concerns it violated federal privacy regulations. Despite this admonition, agency management continued using Spector 360 against the advice of the Inspector General. The Committee found that these tactics, along with adverse personnel decisions, contributed to a climate of fear and intimidation among agency managers and staff.<sup>207</sup>

The Committees' investigation of the FDA's surveillance of whistleblowers raises broader questions about the policies and practices for electronic surveillance at other Executive Branch departments and agencies. In this instance, scientists and doctors raised concerns about the effectiveness of the FDA's process for approving medical devices. Once they learned that scientists and doctors had communicated with Congressional offices and the Office of the Special Counsel, FDA officials did not have a legitimate purpose to institute an intrusive monitoring scheme that would capture those communications, among others. The FDA officials who conducted employee monitoring appeared to be engaged in a form of retaliation, as well as an attempt to interfere with protected whistleblower communications. These actions may have serious ramifications, as they threaten to chill legally protected disclosures to Congress and the Office of Special Counsel. While the FDA has adopted interim policies to regulate surveillance of employees' computers, there are still no permanent guidelines in place. Additionally, the temporary regulations do not provide safeguards to protect whistleblowers from retaliation.

---

<sup>207</sup> Letter from Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform, to Richard A. Lidinsky, Jr., Chairman, Fed. Maritime Comm'n (May 9, 2012).

From the start, when the FDA learned of the potential disclosures to entities outside of the FDA, officials who ordered the monitoring demonstrated an egregious lack of oversight and judgment. There were no guidelines in place, and no one considered the consequences of an invasive monitoring scheme. An agency may not monitor whistleblowers to retaliate against those whose actions were lawful. Here, the scientists and doctors who raised concerns about the FDA's approval process in good faith were within their lawful right to do so.

Testimony from numerous FDA officials established that when officials ordered the surveillance, they failed to consider the legality and propriety of the monitoring. Instead, officials not only approved the monitoring, but also expanded both the number of CDRH employees monitored and the scope of the monitoring. Witnesses also testified that the officials who ordered the monitoring were not adequately aware of the intrusiveness of the computer monitoring software. When FDA officials later contacted OIG to request an investigation into the whistleblowers' release of unauthorized information, OIG declined to investigate because the allegations were unsubstantiated. Despite OIG's response, monitoring of employees continued.

The Committee on Oversight and Government Reform of the U.S. House of Representatives has jurisdiction over the federal civil service, government management, and the management of government operations and activities, as set forth in House Rule X. In addition to its role in conducting oversight and consideration of nominations, the Senate Judiciary Committee also considers other matters, including government information, as set forth in the Standing Rules of the Senate. The Oversight and Government Reform Committee and the Senate Judiciary Committee have a responsibility to ensure federal agencies are using taxpayer dollars appropriately and upholding whistleblower protection laws.

Executive Branch departments and agencies must take a cautious approach to employee monitoring. An intrusive monitoring scheme may run afoul of federal law. In addition, such a scheme could have a chilling effect, making employees reluctant to report waste, fraud, abuse, and mismanagement for fear of retaliation. The Committees will continue to assess whether the FDA is taking adequate steps to prevent such practices from recurring, and will endeavor to determine whether other Executive Branch departments and agencies are taking appropriate steps to engage only in limited employee monitoring when absolutely necessary, subject to thorough vetting and approval.

---

## **XV. Appendix I: Relevant Documents**

---

# Appendix I: Relevant Documents

## URGENT MATTER – REQUEST FOR INVESTIGATION

September 17, 2012

Senator Chuck Grassley  
Ranking Member  
Senate Judiciary Committee  
135 Hart Senate Office Building  
Washington, D.C. 20510

Congressman Darrell Issa  
Chairman  
House Committee on Oversight and Government Reform  
2347 Rayburn House Office Building  
Washington, D.C. 20515

Ms. Carolyn Lerner  
U.S. Special Counsel  
Office of Special Counsel  
730 M Street, N.W., Suite [REDACTED]  
Washington, D.C. 20036

Dear Senator Grassley, Chairman Issa and Special Counsel Lerner:

The National Whistleblowers Center (“Center”) hereby requests a formal investigation into U.S. Food & Drug Administration (“FDA” or “Agency”) violations of the Privacy Act of 1974 (“Privacy Act” or “Act”). *See generally* 5 U.S.C. § 552a(b), (c) and (e). The Center also requests a review of all federal agencies’ compliance with the Act in their implementation of internet security programs and the surveillance of federal employees and private citizens.<sup>1</sup>

These Privacy Act violations relate to the ongoing investigations into the FDA’s targeted surveillance of whistleblowers.<sup>2</sup> Among other violations, the FDA collected and maintained approximately 80,000 pages of records related to employee communications with Congress, the

---

<sup>1</sup> The Center requests these investigations pursuant to the Office of Special Counsel’s (“OSC”) jurisdiction to investigate “gross mismanagement” and violations of law, 5 U.S.C. § 1211, *et seq.*, and Congress’ authority to oversee the actions of the executive branch.

<sup>2</sup> For purposes of clarity, the term “FDA” as used in this letter incorporates the FDA, the Department of Health and Human Services (“HHS”), Quality Associates, and other persons, agencies, or contractors involved in the surveillance program. Managers or attorneys within HHS likely approved FDA’s actions, and various departments within HHS likely participated in or provided support services for the surveillance program. These HHS components must also be fully investigated.

Office of Special Counsel (“OSC”), the Office of Inspector General (“OIG”) and other constitutionally protected communications.<sup>3</sup> The FDA subsequently released these records to the public by posting them on the internet through its contractor, Quality Associates, Inc. (“Quality Associates”).

## **BACKGROUND**

The FDA has a system of records related to the FDA’s targeted surveillance of internal whistleblowers and their associates (“Surveillance Cache”).<sup>4</sup> The Surveillance Cache consists of approximately 80,000 pages of screen shots of the targets computers, intercepted e-mails, e-mail attachments, records taken from privately owned portable hard drives (“thumb drives”), drafts of legal filings with the OSC and OIG, and communications with Congress. Along with the intercepted information, the Surveillance Cache contains internal FDA memoranda regarding the surveillance, and a full index of the intercepts, contained in sixty-seven “logs” (“Log”). Each Log outlines the specific records collected, stored, maintained and disclosed by the FDA, along with the corresponding Bates stamp number.<sup>5</sup>

The FDA collected the Surveillance Cache through spyware programs, including the “Spector” program. Spector permitted the FDA to “capture every single keystroke” the whistleblowers typed on their computers, including passwords. *See* SpectorSoft Brochure, Exh. 1. Spector also permitted the FDA to “read every email sent and received” by the whistleblowers and conduct continuous “Screen Snapshot Surveillance” of “EVERYTHING” the employees did online. *Id.* (emphasis in original).<sup>6</sup>

The records in the Surveillance Cache were culled from likely millions of pages of records obtained through the FDA’s surveillance of its whistleblowers. According to a letter sent to Senator Grassley from the FDA, the surveillance program targeted five whistleblowers’ computers for 11 to 78 weeks:

Robert C. Smith, April 22, 2012 - July 7, 2010 (11 weeks);  
Paul T. Hardy, May 24, 2010 - May 5, 2011 (35 weeks);  
Ewa M. Czerska, June 30, 2010 - December 6, 2010 (23 weeks)  
[REDACTED] June 30, 2010 - November 5, 2010 (18 weeks)

---

<sup>3</sup> The FDA has repeatedly cited to the Federal Information Security Management Act of 2002 (“FISMA”) as the authority for its surveillance program. *See* CDRH 8-24-12 001285. Nothing in FISMA repealed any provision of the Privacy Act or authorizes agencies to violate the Privacy Act in the administration of FISMA. FISMA mandates that federal agencies continue to adhere to the Privacy Act and prohibits agencies from using FISMA as a means to interfere or spy on communications with Congress. *See* 44 U.S.C. § 3549 (“Nothing in this [FISMA] subchapter . . . may be construed as affecting the authority of . . . any agency, with respect to the . . . protection of personal privacy under section 552a of title 5 . . . or the disclosure of information to the Congress . . . .”)

<sup>4</sup> The Center discovered and located the Logs and Surveillance Cache through a Google search.

<sup>5</sup> Copies of the Logs and the underlying documentation will be provided upon request. However, based on the prior availability of these materials on the World Wide Web, we understand that these documents are currently readily available.

<sup>6</sup> The FDA confirmed that it activated these features in a letter to Senator Grassley dated July 13, 2012.

R. Lakshmi Visnvajjala, June 30, 2010 - December 31, 2011 (78 weeks)

*See* Letter, FDA to Grassley, Exh. 2 (July 13, 2012). The letter also indicates that the FDA took a screenshot of the targets' computers every five seconds. In addition, the FDA copied the entire contents of the whistleblowers' hard drives and all connected storage devices—including encrypted thumb drives. The FDA also activated software that records keystrokes and passwords. *Id.*

The full extent of the FDA's systems of records is as of yet unknown. Given the extent of the FDA's surveillance activities, though, it is clear that the 80,000 pages in the Surveillance Cache is a targeted, refined and filtered collection of millions of pages of records of raw surveillance data.

The FDA distributed its Surveillance Cache to various persons, including, but not limited to, its contractor, Quality Associates, Inc. ("Quality Associates"). On or about May 2012, Quality Associates, acting on behalf of the FDA, published the Surveillance Cache on the public internet.<sup>7</sup> A review of the Surveillance Cache demonstrates that FDA officials committed numerous violations of the Privacy Act through its collection, maintenance, and release of these records.

---

<sup>7</sup> Under the Privacy Act, actions taken by FDA contractors are treated as actions undertaken by agency "employees." 5 U.S.C. § 522a(m).

## **SPECIFIC VIOLATIONS OF LAW**

Below is an outline of some of the violations of law documented by the Surveillance Cache, which is in the public record. A full document-by-document review of the Surveillance Cache in light of the requirements of the Privacy Act would result in the documentation of potentially thousands of Privacy Act violations. The full scope of the FDA's surveillance activities is unknown as of yet. Once uncovered though, the Center expects to discover additional Privacy Act violations.

### **I. Violations of the Privacy Act of 1974, § 552a(b)**

The FDA and its officials violated § 552(b) of the Privacy Act of 1974, which states:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record [falls within a number of narrow exceptions].

The FDA disclosed records contained in the Surveillance Cache to agency and non-agency employees who had no need to review the records. For example, the FDA "disclosed" the Surveillance Cache by publishing and making it publicly available on the internet.

Moreover, the Surveillance Cache contained private information concerning whistleblowers and other individuals and agency employees for which there was no justification for collection, maintenance or disclosure. For example, the Surveillance Cache includes attorney-client communications, communications with Congress and the Inspector General, draft Equal Employment Opportunity Commission ("EEO") complaints and numerous highly confidential draft Office of Special Counsel ("OSC") complaints and supporting documents. There was no legal justification for FDA to collect these records, and once collected, there was no legal justification for the disclosure of these records.

We hereby request that each record collected by the FDA, including all of the records published on-line by Quality Associates, be carefully reviewed for actual or potential violations of section 552a(b) of the Privacy Act.

### **II. Violations of the Privacy Act of 1974, § 552a(c)(1)**

The FDA and its officials violated § 552a(c)(1) of the Privacy Act of 1974, which states:

Each agency, with respect to each system of records under its control, shall . . . keep an accurate accounting of--

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under

subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made.

This record-keeping mandate was not followed for the Surveillance Cache. The Surveillance Cache was published in a manner that permitted any person with an internet connection to access these materials at-will with no accounting. Based on the documents produced, and the description of how the FDA processed these documents, it is apparent that the violations of the record keeping requirements of the Privacy Act were not limited to the actions of FDA's contractor. The FDA managers involved in the surveillance program appear to have failed to keep an accounting of their disclosures of records as required under section 552a(c)(1).

The FDA should be required to produce a full accounting of every document collected during its surveillance program and fully document each and every disclosure of these documents, as required under this provision of law. Additionally, as part of the investigation, Quality Associates should be required to document each and every person who accessed the Surveillance Cache on-line in accordance with the requirements of § 552a(c)(1).

The accounting provisions of the Privacy Act are critical for the enforcement of the Act. Without accurate accounting it is impossible to determine whether § 552a(b) was violated, and impossible to determine the nature and scope of harm which may have been caused by the collection, maintenance or distribution of records in violation of the Act. Furthermore, many of the provisions of the Privacy Act can only be followed if an accounting of who accessed the records is accurately maintained.

### **III. Violation of the Privacy Act of 1974, § 552a(e)(1)**

As set forth in this letter, it cannot be reasonably contested that the FDA and its managers violated § 552a(e)(1) of the Privacy Act of 1974, which states:

Each agency that maintains a system of records shall . . . (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President.

This provision is extremely broad. The Act defines "maintain" to include not only the maintenance of an agency record, but also the collection of the record: "[T]he term 'maintain' includes maintain, collect, use or disseminate," 5 U.S.C. § 552a(a)(3).

By maintaining documents related to numerous individuals' communications with OSC, the Office of Inspector General ("OIG"), EEO, and Congress, among others, the FDA maintained thousands of records that were, as a matter of law, not "relevant and necessary" for the FDA to "accomplish a purpose" for which that agency is permitted to engage in. Many other records collected and maintained by the FDA, such as attorney-client communications, cannot,

under any circumstances, meet this standard.

Each record that was collected as part of the whistleblower surveillance program, for which the FDA decided to “maintain,” should be reviewed and a determination made as to how that specific record was both “relevant” and “necessary” for the FDA to “accomplish” its “purpose.” Each and every record “maintained” by the FDA as part of its surveillance program must meet the criteria set forth under § 552a(e)(1). The following document groups are provided as examples of some of the thousands of documents maintained by FDA which fall outside of the records for which FDA could lawfully maintain pursuant to § 552a(e)(1). In this regard, the FDA should provide written justification, under oath, as to the legality of maintaining each and every one of the following records and/or record groupings:

- *Confidential disclosures prepared for the Office of Special Counsel.* Surveillance Cache, Bate Stamped Nos. 52368-56755.
- *Confidential communications with staff members of Congress.* Surveillance Cache, Bate Stamped Nos. 1135-38, 1150, 1180-82, 1186, 1210-14, 1304-14, 1342-46, 1406-08, 1790-98, 1810, 1838-51, 72471-73, 72405-06, 72514-17, 72,522-23.
- *Private communications with EEO Office or Confidential EEO documents.* Surveillance Cache, Bate Stamped Nos. 1282, 1370, 1628-48, 1658-60, 1694-96.
- *Communications with the Office of Inspector General.* Surveillance Cache, Bate Stamped Nos. 65359, 65367-72, 65359, 65367-65372, 65376-412, 65415, 65419-65422.
- *Confidential Draft Letter to Attorney General of the United States setting forth Alleged violations of law.* Surveillance Cache, Bate Stamped Nos. 52173-77.
- *Confidential attorney-client communications related to the terms and scope of representation provided to FDA employees who sought legal representation to file OSC complaints. See e.g.,* Surveillance Cache, Bate Stamped Nos. 509-513 (private attorney-client privileged emails with private attorneys regarding OSC filing).
- *Confidential attorney-client communications related to contacts with Congress and tactic/actions being undertaken in settlement negotiations. See e.g.,* Surveillance Cache, Bate Stamped Nos. 1216-24, 1334.
- *Private communications between whistleblowers in which they discuss the contents of a disclosure to upper-levels of management or whether to raise certain issues to managers.* Surveillance Cache, Bate Stamped Nos. 1318-24, 1382-92.
- *Communications regarding the attempt by one of the whistleblowers {Julian*

*Nicholas] to obtain government employment. Surveillance Cache, Bate Stamped Nos. 803, 813-14, 845-46, 991. These intercepted emails, that were maintained and disclosed by FDA were collected as part of a specific search request to learn about Dr. Nicholas' attempts to obtain employment. See Bate Stamped No. 1016 in which FDA employees conducting the surveillance were instructed to "View All instances" of "correspondence indicating that Julian Nicholas has reapplied to CDRH and is being considered for a position."*

#### **IV. Violations of the Privacy Act of 1974, § 552a(e)(4)**

The FDA violated § 552a(e)(4) of the Privacy Act of 1974, which states:

[Each agency shall] . . . publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include . . . (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records . . . ; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content.

The FDA failed to establish rules governing the "storage, retrievability, access controls, retention, and disposal" of the Surveillance Cache. The FDA had no process to notify the targets of its surveillance program that the agency had created a system of records related to them. The FDA had no process to notify the targets that they had the right to notification and access, or the right to contest the content of this system of records.

For example, Congressional staff members whose private and constitutionally-protected correspondence was collected and maintained by the FDA had a right to notice regarding the storage of these records. The same is true for the numerous FDA employees whose materials were obtained.

This provision of the Privacy Act is essential to ensure that the gross violations of law and privacy caused by the FDA's online publication of the Surveillance Cache would never have occurred. Had the FDA not violated this provision of law, it may have been able to properly police its collection, storage and distribution process.

#### **V. Violations of the Privacy Act of 1974, § 552a(e)(6)**

The FDA violated § 552a(e)(6) of the Privacy Act of 1974, which states:

. . . prior to disseminating any record about an individual to any

person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes.

The FDA disseminated, at the very least, approximately 80,000 pages of records to an outside contractor, which in turn were made publicly available for the world to see on the World Wide Web or internet.<sup>8</sup> Much of the Surveillance Cache was not “relevant for agency purposes” as a matter of law or fact. For example, the OSC materials, which constitute thousands of pages of the information provided to Quality Associates, could not, under any circumstance, be considered records that were “relevant for agency purposes.”

When Quality Associates re-published these records on the World Wide Web, the violations were compounded. As outlined in this letter, FDA’s dissemination of protected communications was not “relevant for agency purposes.” These communications include Congressional communications, attorney-client communications, EEO draft documents, documents describing how persons engaged in First Amendment protected activities, and numerous other records.

## **VI. Violations of the Privacy Act of 1974, § 552a(e)(7) of the Privacy Act**

The FDA violated § 552(a)(7) of the Privacy Act of 1974, which states:

[no agency may] maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

The Surveillance Cache confirms that the FDA collected and maintained thousands of pages of records “describing how” various individuals “exercise(d) rights guaranteed by the First Amendment.”<sup>9</sup> These records include, but are not limited to<sup>10</sup>:

---

<sup>8</sup> Given the nature and scope of the spyware that was utilized by FDA/HHS to conduct surveillance of whistleblowing activities by the FDA employees, it is more than likely that the 80,000 pages represent a small fraction of the documents collected or intercepted by the agency as a result of its surveillance program. Accordingly, the actual number of documents disseminated by the agency could be considerably greater than the 80,000 pages that were published on the internet.

<sup>9</sup> According to the U.S. Department of Justice Privacy Act guidebook: “The OMB Guidelines advise agencies in determining whether a particular activity constitutes exercise of a right guaranteed by the First Amendment to ‘apply the broadest reasonable interpretation.’ 40 Fed. Reg. 28,948, 28,965 (July 9, 1975), available at [http://www.whitehouse.gov/omb/assets/omb/inforeg/implementation\\_guidelines.pdf](http://www.whitehouse.gov/omb/assets/omb/inforeg/implementation_guidelines.pdf); see also 120 Cong. Rec. 40,406 (1974).” DOJ, *Overview of The Privacy Act of 1974 2010 Edition*. All of the examples set forth herein are unquestionably covered under the First Amendment, as they constituted records related to employee speech on matters of “public concern” that were not subject to the “official duty” exception carved out in the case of *Garcetti v. Ceballos*, 547 U.S. 410 (2006).

- Documents related to communications with Congress. *See*, Surveillance Cache, Bate Stamped Nos. 72514-72515 (snapshot recording email from Dr. Czerska to [REDACTED] and [REDACTED] of Senator Grassley’s staff); 72522-72523 (snapshot recording email from Dr. Smith to Dr. Czerska advising her to contact Grassley’s Office, Van Hollen’s Office, and Senate staff member Jack Mitchell); 72405-72406 (snapshot recording of Mr. Hardy’s Computer 8-17-2010 shows email to Joan Kleinman from Congressman Van Hollen’s office); 1838-1851 (snapshot recordings of multiple emails between Dr. Smith and Van Hollen’s office); 72516-72517 (Snapshot Recording of email from Dr. Czerska to Senate staff member Jack Mitchell with attachments complaining about Shuren and Sharfstein); 1154 (file folders permitting FDA to access documents filed for Congressional staff members, including “Joanne” and “Van Hollen;” 1436 (screenshot of computer inbox messages showing emails to Senate staff member Jack Mitchell and Van Hollen staff member “Joan;” 1154 (Snapshot Recording of files saved for various Congressional offices, listing “desktop” folders “For Congress,” “For Emilia” [an aid for Senator Grassley], “For Joanne” [an aid on the House Oversight Committee] and for “Van Hollen.”
- Documents related to communications with the Office of Special Counsel and/or complaints drafted for filing with the OSC. *See* Surveillance Cache, Bate Stamped Nos. 52368-56755 (thousands of pages of OSC filing documents collected, maintained and distributed by FDA); 1720-1721 (Snapshot Recording of Smith computer shows contents of folder named “OSC Filers” that shows the names of all persons planning to file OSC complaints); 509-513 (private attorney-client privileged emails with private attorneys regarding OSC filing); 53271-53273 (copies of confidential scanned signature pages for Dr. Nicholas’ OSC Form 11 filing); 53560-53561 (copies of confidential scanned signature pages for FDA whistleblower Nancy Wersto’s OSC Form 11 filing); 1154 (snapshot of Desktop file folders containing OSC documents entitled “OSC Corrections” and “OSC Individual Folders Final Cruzel.”
- Documents related to communications with the HHS Office of Inspector General. *See* Surveillance Cache, Bate Stamped Nos. 65359, 65367-65372, 65389-65401, 65407-65410, 65419-65422, 65415; 1140: screenshot listing numerous emails with OIG agents Les Hollie and German Melo and other documents related to OIG; 1164: screenshot of document folder established for “HHS OIG.”
- Documents intercepting confidential communications between the FDA scientists and doctors and their attorneys. *See* Surveillance Cache, Bate Stamped Nos. 509-513 (private attorney-client privileged emails with private attorneys regarding OSC filing); Bate Stamped No. 1326 (screenshot of inbox email from attorney

---

<sup>10</sup> The page numbers referenced in this letter are the page numbers placed on these documents either by FDA or Quality Associates. Additional examples of records collected, maintained and/or disclosed by the FDA in violation of § 552a(e)(7) are set forth in the discussion regarding violations of § 552a(e)(1), which also sets forth specific citations to records published on-line by Quality Associates.

marked “STRICTLY CONFIDENTIAL [sic] ATTORNEY CLIENT” and referencing “Office of Special Counsel filing” with a message from the attorney stating “sounds good” [emphasis in original]; Bate Stamped No. 1280 (screenshot of inbox email from “█████” marked “Confidential Attorney-Client Communication”); Bate Stamped No. 1292 (screenshot of inbox email from attorney “████████████████████” referencing “Office of Special Counsel Filing” with a message stating “Great!”).<sup>11</sup>

- Documents intercepting confidential communications related to EEO proceedings. See Surveillance Cache, Bate Stamped Nos. 643-684 (emails with Congressional offices about FDA whistleblower “████████████████████”’s EEO complaint); 558-563 (Czerska email communications with EEO office intercepted); 67320-67321 (Screenshots of emails from Czerska to Smith about her EEO amendment); 1628-1651 (Screenshots of Smith editing Czerska EEO document labeled as ghostwriting); 67454-67460 (Email from Czerska to EEO making complaints against Shuren); 2542-2546 (Email from Smith to EEO Officer “████████████████████” about Smith EEO complaint); 1154 (Snapshot of “Desktop” file folders containing documents for EEO proceedings, marked as “EEO,” “Cindy EEO” and “Julian EEO.”)
- Screenshots of the whistleblowers’ email “in-box” listing who the whistleblower communicated with and a summary of the communication. The “inbox” communications collected and maintained by FDA include: From the Screenshot dated 4/28/10 (page 1264): message sent to “Jack,” a Senate staff member, discussing “HHS OIG investigation,” a message sent from Dr. Nicholas discussing his “EEO formal complaint,” and an email discussing “amendment of EEO complaint;” From the Screenshot dated 5/3/10 (page 1650): “Confidential Attorney Client Communication,” “suggested response to EEO,” “█████bank Service” communication; Screenshot dated 5/12/10 (page 1328): email message between two clients represented by one attorney under a joint representation agreement discussing documents obtained from HHS OIG and the “need” to speak with their attorney “█████” Screenshot dated 5/14/10 (page 1340): numerous emails from “████████████████████” discussing her EEO case, including her communications with Congress, her settlement discussions and offers, and the contents of her complaints; Screenshot dated 5/15/10 (page 1354): “draft email for Joan” (staff member for Congressman Van Hollen), “melo emails” (emails to and from HHS OIG investigator), email to “Jack” (a Senate staff member) concerning the “HHS OIG,” an email from another whistleblower, entitled “Retaliation and Prohibited Personnel Practices at FDA;” Screenshot dated 5/13/10 collecting documents related to “PJ thoughts,” “DOJ,” “Julian EEO,” and “█████ EEO.”

---

<sup>11</sup> Employee communications with attorneys are given special protections under the First Amendment, and are entitled to “rigorous protection.” *Martin v. Lauer*, 686 F.2d 24 (D.C. Cir. 1982). The attorney-client records intercepted by the FDA, and thereafter maintained by the FDA and disclosed directly concerned the fact that the FDA whistleblowers were in the process of hiring attorneys to represent them in OSC filings. Thus, the violations documented in the referenced documents materially compounded the severity of the violations of the Privacy Act.

- The logs published online set forth an index of thousands of documents collected, maintained and distributed by the FDA. Thousands of pages of documents identified in these logs fall within the § (e)(7) prohibition concerning the collection, maintenance and distribution of such documents.

The U.S. Court of Appeals for the District of Columbia Circuit explained the seriousness of these violations:

Similarly, although not expressly provided for in the Constitution, courts have long recognized that “the First Amendment has a penumbra where privacy is protected from governmental intrusion.” *Griswold v. Connecticut*, 381 U.S. 479, 483, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510 (1965). This penumbra of privacy can be invaded, under certain circumstances, by the mere inquiry of government into an individual’s exercise of First Amendment rights. See *Buckley v. Valeo*, 424 U.S. 1, 64, 96 S.Ct. 612, 656, 46 L.Ed.2d 659 (1976) (“compelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment”); *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 544, 83 S.Ct. 889, 893, 9 L.Ed.2d 929 (1963); *Talley v. California*, 362 U.S. 60, 64, 80 S.Ct. 536, 538, 4 L.Ed.2d 559 (1960); *NAACP v. Alabama*, 357 U.S. 449, 461-63, 78 S.Ct. 1163, 1171-72, 2 L.Ed.2d 1488 (1958) (“compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . effective . . . restraint on freedom of association”). **Thus it is not surprising that Congress would have provided in this Act, dedicated to the protection of privacy, that an agency may not so much as collect information about an individual’s exercise of First Amendment rights except under very circumscribed conditions.**

*Albright v. United States*, 631 F.2d 915 (D.C. Cir. 1980) (emphasis added).

The FDA and its responsible officials and contractors committed hundreds or thousands of violations of § (e)(7) based on a review of the Surveillance Cache alone. However, we estimate that the Surveillance Cache is only a sampling of millions of pages of records collected by the FDA pursuant to their spying program. This is a conservative estimate based on public representations of FDA officials regarding the nature and scope of their surveillance program and the technology utilized to intercept and create records of the whistleblowers’ activities. The FDA’s collection, maintenance and/or distribution of a large portion of these documents most likely violates § (e)(7).

We request an investigation of the full and complete extent of these violations, not just the violations that are evidenced by the online activities of Quality Associates.

## **VII. Violations of the Privacy Act of 1974, § 552a(e)(9)**

The FDA violated § 552a(e)(9) of the Privacy Act of 1974, which states:

[Each agency shall] establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.

The FDA admits that commencing on April 22, 2010, it started to collect and maintain records on employee whistleblowers through a highly complex and intrusive warrantless administrative surveillance program. The agency admits that it collected and maintained records on at least five employee “whistleblowers” who had made in constitutionally and statutorily protected speech to a number of appropriate authorities. However the documents published online indicate that at least seven persons were subjected to covert surveillance, and a system of records was created on these seven persons. *See* Surveillance Cache, Bate Stamped No. 1854. An additional 14 persons were eventually viewed as “collaborators” with the main whistleblowers. *See* Surveillance Cache, Bate Stamped Nos. 1023-1024.

The FDA created this system of records in or about April 2010 without implementing the mandatory quality assurance requirements of the Privacy Act. There appears to have been no “rules of conduct” published by the agency controlling the behavior of persons involved in this program. There appears to be no “rules” governing the design of the record collection process. Had such rules been implemented, perhaps the agency would not have willfully and aggressively collected confidential documents covered under the § (e)(7) exception, and if collected would not have distributed such documents to outside contractors and would not have had those documents published on the World Wide Web.

There appears to have been no “instructions” given to the persons responsible for designing, developing, operating and maintaining the system of records created by the surveillance program.

## **VIII. Violations of the Privacy Act of 1974, § 552a(e)(10)**

The FDA violated § 552a(e)(10) of the Privacy Act of 1974, which states:

[Each agency shall] establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

The FDA’s violation of this provision is extremely troublesome and threatens the

financial security of the whistleblowers who were the subject of the targeted surveillance.

Specifically, as part of its surveillance program, the FDA purchased and authorized the targeted use of the highly-intrusive Spector spyware to collect and maintain records on suspected whistleblowers and their “collaborators.” It is clear from a review of the documents FDA published online, through its contractor Quality Associates, that the FDA failed to ensure that the system of records created with the use of the Spector program contained “appropriate administrative, technical and physical safeguards” that would “insure the security and confidentiality of records.”

The Spector program permitted FDA to collect highly-personal information regarding its employees, including financial and medical data and private passwords to the employees’ personal third-party email and financial accounts. The FDA was able to obtain full access to the whistleblower-employee’s highly confidential personal financial information, and it had secret access to the codes necessary to effectuate financial transactions from the employee’s private bank and retirement accounts.

Thus, FDA officials and unknown other employees or contractors had ready access to password-protected financial data, and were in a position to use this information to engage in fraud.

A brief look at a handful of screenshots published online by Quality Associates demonstrates that FDA had access to the personal financial information of the targeted whistleblowers. For example:

- Surveillance Cache, Bate Stamped No. 1454 (Private Citibank Email);
- Surveillance Cache, Bate Stamped No. 1472 (Capital One statement)
- Surveillance Cache, Bate Stamped No. 1368 (Citibank Debt Card email)
- Surveillance Cache, Bate Stamped No. 1164 (an AZA Transfer of Funds transaction conducted by email);
- Surveillance Cache, Bate Stamped No. 1292 (email from Vanguard re: investment newsletter);
- Surveillance Cache, Bate Stamped No.: 73660 (email transactions with Mint.com, including loan serving transactions, fees charged to Citibank account, fees charged to HSBC account, and weekly financial summaries).

## **IX. Violations of the Privacy Act of 1974, § 552a(m)**

The FDA violated § 552a(m) of the Privacy Act of 1974, which states:

When an agency provides by a contract for the operation by or on

behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

This provision mandates that any investigation into FDA's misconduct also include a full investigation into the actions of FDA's contractor, Quality Associates.

## **X. Violation of the Privacy Act Requirements of the Federal Acquisition Regulations**

The FDA entered into a contract with Quality Associates to maintain and distribute Privacy Act protected documents. Under the provisions of the Federal Acquisition Regulations ("FAR"), 48 C.F.R. § 24.104, FDA must ensure that Quality Associates "design, development," and "operat[e]" its record keeping systems in conformance with the Privacy Act. Based on the public disclosure of the Surveillance Cache, the FDA and / or Quality Associates violated the Privacy Act provisions of the FAR.

### **REQUEST FOR INVESTIGATION PURSUANT TO 5 U.S.C. § 1213**

The National Whistleblowers Center hereby requests an investigation of the FDA and Quality Associates. Under the Whistleblower Protection Act, the U.S. Special Counsel has broad jurisdiction to investigate agency misconduct, including violations of law and gross mismanagement. *See* 5 U.S.C. §1211, *et seq.* As set forth above, the FDA grossly mismanaged its obligations under the Privacy Act and violated the statutory requirements of the Act, resulting in systemic violations of the legal, statutory and constitutional rights of FDA employees.

In addition, a careful investigation must be conducted into how and why FDA collected, maintained and disclosed records related to the whistleblowers' intent to file complaints with the OSC. All such complaints are required to be kept confidential as a matter of law, and under the Privacy Act FDA could not lawfully collect, maintain or disclose such records.

The FDA's actions undermine federal workers' willingness to approach Congress, the OSC, and the OIG by destroying the presumption of confidentiality. For example, in one intercepted e-mail, an FDA worker explains why she was reluctant to file an OSC complaint: "Filing will make people really unhappy . . ." In response, her correspondent explains that OSC filings are confidential: "The names of the persons who file are secret . . ." *See* Surveillance Cache, Bate Stamped Nos. 1290.<sup>12</sup>

Subsequently, the FDA published her identity and her affiliation with the whistleblower

---

<sup>12</sup> The cited document is a screenshot taken contemporaneous with the drafting of the email, and is not the finished document. FDA apparently thought this communication was very significant, as it separately collected and maintained the final version of the email. Surveillance Cache, Bated Stamped No. 579.

group. With the FDA's release of these records, it is now well known and notorious that communications with OSC, OIG, and Congress have no guarantee of secrecy nor confidentiality.

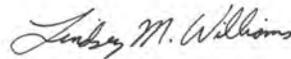
The Surveillance Cache should never have been collected, maintained or distributed.<sup>13</sup> In particular, interception of OSC, Congressional, and OIG-related records and communications should not be tolerated. Any violations should be subject to the strictest sanction.

Thank you in advance for your prompt attention to these matters. Should you need any additional information, please do not hesitate to contact us by phone at (202) [REDACTED].

Respectfully submitted,

NATIONAL WHISTLEBLOWERS CENTER

By:



Lindsey M. Williams  
Director of Advocacy and Development  
National Whistleblowers Center

---

<sup>13</sup> Although this employee's name was widely disclosed by FDA, in order to minimize the harm caused by FDA's violation of law, we ask that you not publicly release this person's identity.



DEPARTMENT OF HEALTH AND HUMAN SERVICES

MEMORANDUM

Food and Drug Administration  
Office of Device Evaluation  
9200 Corporate Boulevard  
Rockville, MD 20850

October 14, 2008

Congress of the United States  
House of Representatives  
Representative John D. Dingell  
2328 Rayburn House Office Building  
Washington, DC 20515

Dear Mr. Dingell:

This letter seeks your urgent intervention because serious misconduct by managers of the U.S. Food and Drug Administration (FDA) at the Center for Devices and Radiological Health (CDRH) is interfering with our responsibility to ensure the safety and effectiveness of medical devices for the American public and with FDA's mission to protect and promote the health of all Americans. Managers at CDRH have failed to follow the laws, rules, regulations and Agency Guidance to ensure the safety and effectiveness of medical devices and consequently, they have corrupted the scientific review of medical devices. This misconduct reaches the highest levels of CDRH management including the Center Director and Director of the Office of Device Evaluation (ODE).

██████████ physicians and scientists ██████████ at CDRH have already sought intervention from the FDA Commissioner. The physicians and scientists ██████████ are responsible for ensuring the safety and effectiveness of all ██████████ devices before they are used on the American public. The devices we regulate are crucial and fundamental to medical practice ██████████

██████████ devices constitute a substantial ██████████ cost to the ██████████ American health care system with more than 500 million adult and pediatric ██████████ procedures performed every year in the United States.

It is crucial for FDA to regulate medical devices based on rigorous science. As stated in the November 2007 FDA Science Board Report<sup>1</sup> entitled "FDA Science and Mission at Risk":

<sup>1</sup> Available at [http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b\\_02\\_00\\_index.html](http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b_02_00_index.html)

“A strong Food and Drug Administration (FDA) is crucial for the health of our country. The benefits of a robust, progressive Agency are enormous; the risks of a debilitated, under-performing organization are incalculable. The FDA constitutes a critical component of our nation’s healthcare delivery and public health system. The FDA, as much as any public or private sector institution in this country, touches the lives, health and wellbeing of all Americans and is integral to the nation’s economy and its security. The FDA’s responsibilities for protecting the health of Americans are far-reaching. ... The FDA is also central to the economic health of the nation, regulating approximately \$1 trillion in consumer products or 25 cents of every consumer dollar expended in this country annually. The industries that FDA regulates are among the most successful and innovative in our society, and are among the few that contribute to a positive balance of trade with other countries. The importance of the FDA in the nation’s security is similarly profound. ... Thus, the nation is at risk if FDA science is at risk.”

There is extensive documentary evidence that managers at CDRH have corrupted and interfered with the scientific review of medical devices. The scientific review of medical devices is required to work as follows: FDA clinical and scientific experts (“FDA experts”) review submissions based on the best available scientific information and in accordance with the Food Drug and Cosmetic Act, the Code of Federal Regulations and Agency Guidance documents (when such Guidance documents exist for a particular device or category of devices). FDA experts give their best scientific judgments, opinions and conclusions regarding safety and effectiveness of medical devices and make corresponding regulatory recommendations. These form the scientific and regulatory basis for managers at FDA to make final regulatory decisions (i.e., clearance or approval of medical devices). While managers can disagree with FDA experts, they cannot order, force or otherwise coerce FDA experts to change their scientific judgments, opinions, conclusions or recommendations. In accordance with the law, if managers at FDA disagree with FDA experts, managers must document their disagreements in official Agency records, must scientifically justify any contrary judgments, opinions, conclusions or recommendations and must take personal responsibility for their final regulatory decisions. The review process is well described in long existing Agency Guidance.<sup>2</sup>

The law requires that qualified experts make safety and effectiveness determinations based on valid scientific evidence. Managers at CDRH with no scientific or medical expertise in [REDACTED] devices, or any clinical experience in the practice of medicine [REDACTED], have ignored serious safety and effectiveness concerns of FDA experts and have ignored scientific regulatory requirements. To avoid accountability, these managers at CDRH have ordered, intimidated and coerced FDA experts to modify their scientific reviews, conclusions and recommendations in violation of the law. Furthermore, these managers have also ordered, intimidated and coerced FDA experts to make safety and effectiveness determinations that are not in accordance with scientific regulatory requirements, to use unsound evaluation methods, and accept clinical and technical data that is not scientifically valid nor obtained in accordance with legal requirements, such as obtaining proper informed consent from human subjects. These same

---

<sup>2</sup> Available at <http://www.fda.gov/cdrh/g93-1.html>.

managers have knowingly avoided and failed to properly document the basis of their decisions in official Agency records.

Under the banner of regulatory “precedent,” managers at CDRH have demanded that physicians and scientists review regulatory submissions employing methods, and accepting evidence and conclusions, that are not scientifically proven and clinically validated. These demands appear to be based on the misguided notion that because flawed methods, evidence and conclusions were used or accepted in the recent or even the remote past, we must continue to blindly and knowingly accept these flawed methods, evidence and conclusions and continue to use them as the basis for regulatory recommendations. Such invalid regulatory “precedent” goes against current scientific and clinical evidence. Rather than remedy past regulatory or scientific errors after they come to light, and rather than applying the best and latest scientific knowledge and methodology, these managers at CDRH knowingly continue to make the same regulatory and scientific mistakes over and over again. Rather than recall, re-evaluate or otherwise deal with potentially unsafe or ineffective devices that are already on the market, these managers at CDRH continue to approve more devices of the same kind in a non-transparent and non-scientific manner. This is especially true of the 510(k) program but also applies to the PMA program as well as the advice and guidance given to manufacturers before they make regulatory submissions. The practices described above represent an unwarranted risk to public health and a silent danger that may only be recognized after many years.

When physicians and scientists have objected to the management practices described above, managers at CDRH have engaged in reprisals and ignored these critical concerns. FDA physicians and scientists therefore contacted the Office of the Commissioner:

- On May 31, 2008, [REDACTED] FDA physicians and scientists [REDACTED] wrote to the FDA Commissioner, Dr. Andrew von Eschenbach (See attached letter).
- The Commissioner immediately asked Mr. William McConagha, the Assistant Commissioner for Integrity and Accountability, to begin a full investigation.
- Since early June 2008, FDA physicians and scientists have met with Mr. McConagha numerous times and have facilitated his investigation by providing written documentary evidence including internal emails, reviews, memos, meeting minutes, etc.
- Mr. McConagha has characterized the documentary evidence as “compelling,” “convincing” and “sufficient” to justify curative and disciplinary actions. As a result, the Commissioner met with the CDRH Director in August.
- On September 3, 2008, [REDACTED] FDA physicians and scientists [REDACTED] met with the Director of CDRH in the presence of representatives from the Commissioner’s Office. At the request of Mr. McConagha, the FDA physicians and scientists presented the issues and documentary evidence to the Director of CDRH (See attached presentation).

- The Director of CDRH then conducted his own investigation and concluded that we, FDA physicians and scientists, need to “move forward,” thus allowing managers to avoid and evade any accountability and without taking any curative or disciplinary actions whatsoever. The Director of CDRH has further aggravated the situation by knowingly allowing a continuation of management reprisals. These reprisals now include removal and threatened removal of physicians and scientists [REDACTED] [REDACTED] [REDACTED] as well as illegal and improper employee performance evaluations.
- On September 29, 2008, [REDACTED] FDA physicians and scientists wrote a second letter to Dr. von Eschenbach (see attached letter).

To date, despite involvement by the Commissioners Office, there has been enormous internal resistance from entrenched managers at CDRH including the Center Director and the Director of ODE. These managers seem far more concerned about ensuring their current positions and protecting and promoting their own careers and those of their cronies, than they are about ensuring the safety and effectiveness of medical devices and protecting and promoting the health of all Americans. CDRH managers prefer to employ regulation-based “pseudo-science” rather than science-based regulation.

It is evident that managers at CDRH have deviated from FDA’s mission to identify and address underlying problems with medical devices before they cause irreparable harm, and this deviation has placed the American people at risk. Given the large number of [REDACTED] [REDACTED] submissions to the FDA, the complexity of the scientific and medical issues involved and the importance of [REDACTED] devices to the practice of medicine, we believe that proper regulation of [REDACTED] devices requires the establishment of a new and separate Office at FDA [REDACTED]. This Office must be staffed by expert physicians and scientists at all levels including management and must provide vision and leadership by being proactive rather than reactive, by incorporating the latest scientific and technological evidence into device evaluation, compliance and post-market surveillance, and by making all regulatory decisions in a transparent manner based on sound scientific and clinical principles. At the same time, there is a need for new legislation that modernizes the regulatory structure of the 510(k) program so that complex medical devices are not allowed onto the market without a comprehensive (or in some cases, any) clinical evaluation of their safety and effectiveness. This is especially true for [REDACTED] devices due to their markedly increased use in clinical practice and because [REDACTED] devices employ highly complex hardware and software, undergo rapid technological changes and touch the lives of so many patients on a daily basis. The current framework for medical device adverse event reporting does not work for many [REDACTED] devices [REDACTED] as the adverse effects of [REDACTED] devices are rarely detected immediately, are not transparent on an individual patient basis, and can only be prevented by a rigorous pre-market evaluation process.

FDA leaders need to re-establish the trust of the American people. Congress needs to ensure that FDA physicians and scientists can do their jobs by being allowed to follow the laws, rules and regulations without fear of reprisal, by applying the best and latest scientific knowledge and methodologies, by having an updated modern regulatory structure, and by allocating sufficient financial and other resources to FDA.<sup>1</sup> Finally, FDA leaders and Congress must restore compliance with the law, must hold accountable those managers at FDA that fail to carry out the

FDA mission to protect and promote the health of all Americans, and must protect FDA physicians and scientists so that they can protect the American public.

As the Branch of government responsible for oversight of the FDA, we urgently seek your intervention and help.

[REDACTED]

[REDACTED]

[REDACTED]



JUL 16 2012

Food and Drug Administration  
Silver Spring, MD 20993

JUL 13 2012

The Honorable Darrell Issa  
Chairman  
Committee on Oversight and Government Reform  
House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your letter of February 9, 2012, requesting information about the use of computer monitoring by the Food and Drug Administration (FDA or the Agency) to investigate the illegal and unauthorized release of confidential information related to medical device applications and submissions.

In connection with this matter, there are several cases in active litigation and open investigations by the U.S. Office of Special Counsel (OSC). Further, on June 14, 2012, in response to a request from OSC, the Secretary of Health and Human Services (HHS) asked the HHS Office of Inspector General (OIG) to conduct an investigation of the premarket review process for some medical device applications and submissions, which, in part, relate to the aforementioned unauthorized disclosures. The litigation, OSC investigations, OIG referral, and commensurate need to understand all the facts surrounding the improper disclosure of confidential information, and the subsequent Agency response, require a thorough and deliberate review of events. This review must respect the rights of individual employees as well as protect governmental legal prerogatives. Such constraints might limit the Agency's response to questions related to matters involved in the litigation and open investigations. Please accept my apology for the delay in responding due to the pending investigations and litigation related to this matter.

FDA recognizes and appreciates the Committee's legitimate oversight interest in the issues raised in your letter. We share your concern that our employees be afforded all appropriate and available opportunities to raise issues relating to Agency policies and decisions. At the same time, FDA has important obligations to ensure the integrity of the medical device premarket review process, which requires FDA, including the Center for Devices and Radiological Health (CDRH), to routinely receive and review trade secrets and confidential commercial information submitted by regulated entities, the disclosure of which could cause competitive harm to the company submitting the information. Congress has enacted statutes that expressly prohibit FDA personnel from disclosing trade secrets and confidential commercial information. Such unauthorized disclosures not only violate federal law and undermine the integrity of FDA programs; they also can result in civil suits against FDA and/or criminal and monetary penalties against its employees. In many instances, the mere fact that a device firm has submitted a pre-market submission or application is itself confidential. Similarly, details about a company's

product in development, or the data and information concerning a product's safety and effectiveness, could give the company's competitors an unfair advantage by providing previously unavailable insights into the development process, and disclosure of such details could undermine incentives for innovation and competition in the commercial market. Protection of this highly sensitive information is of utmost importance to FDA.

Please note that this response may include information that is trade secret, commercial confidential, or other information otherwise protected from disclosure to the public, for example under the Freedom of Information Act (5 U.S.C. § 552), the Trade Secrets Act (18 U.S.C. § 1905), the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 331(j)), and Agency regulations. We respectfully request that the Committee not publish such information in order to preserve the proprietary and competitive interests of the companies involved, as well as other significant interests. FDA staff would be pleased to discuss with Committee staff the protected status of any specific information.

Please also note that this letter reflects FDA's current understanding of the facts pertaining to this matter and is based upon the Agency's review of the matter to date.

FDA construes the questions in your letter to relate to the individuals who were signatories to the January 2009 letter to which your letter refers, as well as to Lakshmi Vishnuvajjala, who, though not a signatory, was one of the five individuals whose computer activity was monitored by FDA pursuant to the Agency's investigation into suspected unauthorized disclosures by CDRH personnel.

We have restated your specific questions below in bold, followed by our responses.

**1. Identify the individual(s) responsible for deciding to initiate monitoring of the personal e-mail accounts of the FDA Nine.**

In 2009 and 2010, FDA became aware of a series of unauthorized disclosures of confidential information contained in various medical device premarket applications and submissions under review. For instance, on January 13, 2009, *The New York Times (Times)* published an article that included confidential information from iCAD's then-pending premarket approval application (PMA) for its SecondLook Digital Computer-aided Detection for Mammography device. According to information iCAD provided to FDA, the article's author informed the company that he had received "internal FDA documents" regarding the device from "Scientific Officers of the FDA." On January 13, 2009, legal counsel for iCAD sent a letter to the CDRH Ombudsman expressing concern regarding the apparent disclosure by FDA of the company's confidential PMA information. The January 13, 2009, *Times* article also quoted from an internal Agency memorandum regarding the pending review of Shina Systems' submission seeking clearance to market its AngioCt device. A consultation review memorandum on the premarket notification submission (referred to as a "510(k)") had been written on March 14, 2008, by other CDRH personnel to [REDACTED], a CDRH staff fellow, and Dr. Robert Smith, an FDA medical officer.

Then, on April 16, 2010, CDRH received a letter from legal counsel for GE Healthcare Inc., alleging that FDA had disclosed to the press confidential information from the firm's premarket notification submission for a new CT colonography screening indication for its CT Colonography II image analysis software visualization device. The letter referenced a March 28, 2010, *Times* article as evidence that confidential information from the company's 510(k) submission had been leaked to the press in violation of federal law, FDA regulations, and internal Agency policy. This article referred to "[s]cores of internal agency documents made available to The New York Times." Although the article did not disclose the source of the internal agency documents, it included quotes from both Dr. Robert Smith and former FDA contractor, Dr. Julian Nicholas. The firm requested that FDA "conduct an internal investigation into how this information was leaked to the press."

The question of the authorization of monitoring is being addressed in the OSC investigation you and Senator Grassley have requested, as well as the pending litigation, and the Agency is still identifying and gathering evidence with respect to these issues.

We can assure you, however, that the Agency did not monitor these individuals' use of non-government-owned computers. To the extent an individual elected to use a government computer to engage in correspondence using a personal e-mail account, data derived from such use were collected in the same manner as were data derived from other uses of the government-issued computer.

**2. Identify each employee who was the subject of any form of surveillance, including, but not limited to, screen captures and e-mail monitoring.**

FDA authorized active monitoring of the use of government-owned computers by the following individuals: Ewa Czerska, Paul Hardy, [REDACTED], Robert Smith, and Lakshmi Vishnuvajjala.

**3. State the date on which surveillance started for each employee identified above.**

Software-enabling active monitoring of computer activity was installed by FDA as follows:

- Robert Smith – April 22, 2010
- Paul Hardy – May 24, 2010
- [REDACTED] – June 30, 2010
- Ewa Czerska – June 30, 2010
- Lakshmi Vishnuvajjala – June 30, 2010

As listed above, software-enabling computer monitoring was installed on Dr. Smith's government-issued computer on April 22, 2010—five days after FDA received the GE Healthcare letter alleging unlawful public disclosure of confidential information. During the course of monitoring Dr. Smith's use of his government-issued computer, evidence was uncovered suggesting that certain additional CDRH personnel were participating in unauthorized

disclosures of information, and monitoring was expanded to include these additional personnel, as noted above.

Although your letter states that “[t]he first documented interception of an e-mail occurred in January 2009,” this is incorrect. As indicated above, in no case were any of these individuals subject to computer monitoring prior to April 22, 2010. Screenshots of e-mails that were originally sent or received prior to the date on which monitoring was initiated could only have been captured as a result of the individual having opened or reopened the e-mail message on his/her FDA computer after the date monitoring was commenced.

**4. For any individual no longer employed by FDA whose e-mail was monitored, please explain the circumstances of departure from the agency, including relevant dates.**

- [REDACTED] was a General Schedule employee who was removed from her position on April 29, 2011, for unauthorized disclosure of confidential information. Pursuant to an agreement recently reached between OSC and both HHS and FDA, [REDACTED] has been temporarily reappointed with pay through July 31, 2012.
- [REDACTED] was a Commissioned Corps officer within the U.S. Public Health Service, who was not recommended for promotion by the Annual Promotion Board in September 2011. On October 9, 2011, he was terminated from the Regular Corps pursuant to 42 U.S.C. § 211(g).
- [REDACTED] was at FDA as a limited-term staff fellow appointed pursuant to 42 U.S.C. § 209(g). Her term appointment expired on November 6, 2010.
- [REDACTED] was a Schedule A Appointment Medical Officer. His term appointment expired on July 31, 2010.

**5. Explain the extent of the agency’s surveillance of the FDA Nine, including a description of the methods for and frequency of any surveillance.**

As noted above, FDA collected data regarding certain personnel’s use of their government-owned computers. For each of the individuals subject to computer monitoring, data were collected from the following sources:

- Screenshots, taken every five seconds, of the totality of whatever was visible on one or more monitors in use for a given government-issued computer;
- All e-mail sent or received to/from a given government-issued computer;
- All network activity to/from the government-issued computer;
- All data stored on and printed from the government-issued computer or an external storage drive connected thereto; and
- All keystrokes performed on the government-issued computer.

According to individuals involved at the time, as well as our review of the matter to date, the data collected were searched to identify records of correspondence leaving the FDA network in which the e-mail or any attachment to it contained the term “colonography” or the letter “k” immediately followed by a series of numbers, the latter being intended to identify reference to specific 510(k) premarket notification submissions as to which FDA had received complaints about improper disclosures of confidential information. Later, the search parameters were broadened to include terms beginning with the letter “p” or “g,” followed by a series of numbers, which would potentially correspond to premarket approval device applications or investigational device exemption applications, respectively. Search terms were also eventually expanded to include the names and manufacturers of products about which it was suspected unauthorized disclosures may have been/or were being made. FDA also endeavored to identify e-mails being sent to individuals outside the FDA network that appeared to include confidential Agency records.

FDA is not aware of any information that suggests that Agency personnel collected passwords for individuals’ personal e-mail accounts. According to the forensic engineer principally involved in the computer monitoring, to the extent individuals’ passwords may have been captured, it would have been incidental to the objective of the monitoring and FDA did not utilize or otherwise take any action related to such passwords.

To the extent FDA became aware of the use of personal e-mail accounts to transmit information, it was either through the identification of screenshots, which in many cases recorded correspondence that had been accessed on an FDA computer, or because the individual used his or her FDA e-mail account to send Agency records to his or her own personal e-mail address. It should be noted that once monitored individuals transmitted Agency records to their own personal e-mail account, in many cases the records were almost immediately forwarded further to individuals outside the government.

Note that since 2009, all users of the FDA computer network have received notice upon logging into an FDA computer that they should have no reasonable expectation of privacy when utilizing the FDA computer system.<sup>1</sup>

---

<sup>1</sup> For example, upon logging on to the FDA network, users immediately receive the following warning message:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information, you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

**6. State the purpose of the agency’s surveillance of the FDA Nine.**

FDA initiated monitoring of the government-owned computers of the five individuals identified above for two principal purposes: 1) to identify the source of the unauthorized disclosures, if possible; and 2) to identify any further such unauthorized disclosures so as to better enable FDA to facilitate their cessation.

Your letter states that “it appears that FDA targeted these employees for surveillance because they talked to Congress.” Beginning as early as October 2008, FDA had begun receiving letters and other inquiries from multiple Congressional offices regarding concerns brought to them by various members of the group of individuals you reference. These inquiries made clear that CDRH personnel were seeking the intervention of Congress. Nonetheless, it was not until approximately 18 months after FDA began to receive such inquiries that the monitoring of Dr. Smith’s government-owned computer activity was initiated. The impetus for the monitoring was not any communication to Congress. Rather, the impetus for monitoring was the March 2010 *Times* article and the receipt of the GE Healthcare letter just prior to the initiation of monitoring, which indicated that the preceding pattern of similar unauthorized disclosures of confidential information from other pending medical device applications and submissions was continuing unabated. It should also be noted that, in conducting the computer monitoring, data were collected without regard to the identity of the individuals with whom the user may have been corresponding.

**7. Explain the legal justification relied on by FDA to initiate surveillance of the FDA Nine.**

As explained above, this matter is the subject of current litigation. It should be noted, however, as described above, that since 2009 all users of the FDA computer network have received notice upon logging in that they should have no reasonable expectation of privacy when utilizing the FDA computer system. Please see footnote 1 for the text of the information that all users receive.

You have also requested documents, and we have restated below your requests, followed by our responses.

**1. Documents referring or relating to the FDA Nine collectively or individually, including, but not limited to, all communications to or from Gregory Campbell, Dr. Jeffrey Shuren, Ruth McKee, Ralph Tyler, or Dr. Joshua Sharfstein.**

- 
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

The above warning has been in continuous use since at least September 2010, and a similar warning was in use at the time the monitoring, as described herein, was initiated. Additionally, all FDA personnel are required to receive Computer Security Awareness Training annually, during which they are reminded, among other things, that all network activity may be monitored. The employees about whom you have inquired received such annual training.

FDA is continuing to gather responsive documents, which will be provided in a rolling production.

**2. Documents created or obtained as a result of e-mail monitoring since January 1, 2009, including but not limited to all documents in the file named “FDA 9.”**

As noted above, FDA did not commence the computer monitoring discussed above until various dates in 2010. The Agency is continuing to gather responsive documents, which will be provided in a rolling production.

**3. Guidance from the Office of the General Counsel referring or relating to monitoring employee e-mail accounts.**

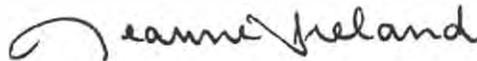
We are working to identify any documents that may be responsive to this request.

**4. Guidance from the Office of the Inspector General referring or relating to monitoring employee e-mail accounts.**

We are not aware of documents provided to FDA by OIG that provide general guidance, with respect to the monitoring of employee e-mail accounts.

Thank you, again, for contacting us concerning this matter. If you have further questions, please let us know.

Sincerely,

A handwritten signature in black ink that reads "Jeanne Ireland". The signature is written in a cursive style with a large initial "J".

Jeanne Ireland  
Assistant Commissioner  
for Legislation

cc: The Honorable Elijah E. Cummings  
Ranking Member  
Committee on Oversight and Government Reform

## Interim Report of Investigation

To: Lori Davis, Chief Information Officer  
CC: Joe Albaugh, Chief Information Security Officer  
From: Joe Hoofnagle, Incident Response and Forensic Lead; Christopher Newsom,  
Incident Response and Forensic Investigator  
Date: June 3, 2010  
Subject: Interim Report of Investigations - Robert C. SMITH

---

In May of 2010 specific allegations were presented to the FDA Security Department regarding Robert C. SMITH, Medical Officer - CDRH/ODE/DRARD. These allegations pertained to the following:

- Ghost writing HIS subordinates' reports, in particular those surrounding those reports that are identified by the letter "K" followed by six (6) numbers.
- SMITH communicating with external news sources (press) regarding HIS concerns over the FDA's approval process of particular medical devices surrounding CT scans and colonography. This allegation particularly related to Gardiner Harris, reporter for the New York Times.

The Security Department has initiated a review of FDA data sources associated with SMITH to determine the validity of the allegations. The analytical findings to date appear to support the allegations, however the review is ongoing and substantial volumes of data are currently being culled.

The subordinate information that follows contains:

- FDA personnel that appear to be involved with the allegations,
- Communications with external press sources, including Gardiner Harris, reporter for the New York Times,
- Collaboration amongst FDA personnel and external sources to provide defamatory information about the FDA approval process as well as issues regarding hostile work environment and discrimination,
- Distribution of potentially sensitive information to external, non FDA sources, and
- Information indicating potential involvement of Congress member(s) serving as conduits to the press.

Interim Report of Investigations - Robert C. SMITH

Subjects of Interest ..... 3  
    Primary Subjects ..... 3  
    Secondary Subjects ..... 3  
    Ancillary Subjects ..... 4  
    Media Outlet Subjects..... 4  
Interim Report of Analysis & Findings ..... 6  
    Allegation 1: Ghost Writing ..... 6  
    Allegation 2: Supplying Internal Documents and Information to External Sources..... 6  
    Possible Future Concerns: ..... 7  
    Possible Potential Issue: ..... 8  
    Possible Collaboration Issue:..... 8

## Interim RCS Report of Analysis & Findings

\* Underlined items indicate findings post “Preliminary RCS Analysis Results.doc”

### Allegation 1: Ghost Writing

- Indications of RCS receiving documents and email from co-workers / co-complainants pertaining to investigation via FDA email and Gmail
- Documents being edited by RCS and returned via Gmail – Mostly investigation related documentation.
- Lengthy suggestions of content to be used supplied by RCS via Gmail. These are contained in body of email for use by recipients (co-workers / co-complainants)
- Documents being edited by RCS and returned via Gmail – Identified Device Review documents/correspondence.
- Many of the above referenced documents and communications are currently going to JN for review/input.
- JN currently heavily involved in communications regarding investigation

View All possible instances of the above allegation in order by date

### Allegation 2: Supplying Internal Documents and Information to External Sources

- Multiple Gmail contacts with Gardiner Harris – NY Times  
Identified multiple Gmail communications between RCS and Gardiner Harris regarding telephonic communications and in-person meetings

View All instances of the above noted in order by date

- Multiple Gmail contacts with Matthew Perrone – Associated Press News  
Identified multiple Gmail communications between RCS and Gardiner Harris regarding telephonic communications and in-person meetings

View All instances of the above noted in order by date

- Multiple Gmail contacts with Alyah Khan – Inside Washington Publishers news organization
  - RCS Received internal document via Gmail from Kahn reference Chris Van Hollen – Alyah requested in same email not to be revealed as source or distribute document.

View All instances of the above noted in order by date

- RCS currently assisting Khan with editing story regarding Chris Van Hollen

View All instances of the above noted in order by date

- Kahn indicates the “editor” wants to hold the “Van Hollen story” as of May 14, 2010

View All instances of the above noted in order by date

- RCS and JN are in communication with Kahn regarding articles

View All instances of the above noted in order by date

- RCS and JN are in communication with Robert Lowes (Unknown News Org) may be an associate of Kahn’s

View All instances of the above noted in order by date

- Multiple Gmail contacts with Joe Bergantino and Rochelle (unk last name) - RCN Cable Washington based Direct Cable provider)  
Identified multiple Gmail communications between requesting times to meet and talk.

View All instances of the above noted in order by date

- RCS and JN received communication from Lainey Moseley – (Philadelphia Journalist of Unknown News Org) – Looking for a “Bigger Story” on CT scans, patient safety and FDA recommendations.

View All instances of the above noted in order by date

- Multiple Gmail contacts with Ned Feder (POGO – Project On Government Oversight – non affiliated non profit) – Emails include attachments with significant amount of documents.

View All instances of the above noted in order by date

- Multiple Gmail contacts with Jack Mitchell (aging.senate.gov) – Emails include attachments with significant amount of documents including those self-redacted.

View All instances of the above noted in order by date

- Multiple Gmail contacts with JN – Emails include attachments with significant amount of documents including those self-redacted

View All instances of the above noted in order by date

- Multiple Gmail contacts with Joan Kleinman (District Director for Rep. Chris Van Hollen) – Emails include attachments with significant amount of documents including those self-redacted.

View All instances of the above noted in order by date

### **Possible Future Concerns:**

- Gmail from Paul Hardy stating “Time to pound them into dust – I think its time to talk to Joe about the documentary on Frontline” – Received May 11, 2010 - (Joe is an unknown person)

View All instances of the above noted in order by date

- Gmail correspondence indicating that Julian Nicholas has reapplied to CDRH and is being considered for a position.

View All instances of the above noted in order by date

### **Possible Potential Issue:**

- Gmail correspondence with outside physician(s) - Possible FDA research knowledge being leveraged (ref CON and STARK) CSIRT not sure whether or not is these are FDA internal projects.

View All instances of the above noted in order by date

- Image of Certificate of Remittance (transfer) from Shinan Bank dated 4/15/09 viewed on 4/26/2010

View All instances of the above noted in order by date

**Possible Collaboration Issue:**

- Numerous FDA emails and Gmail amongst primary and secondary actors indicating collaborative correspondence regarding review, editing, compilation, production or distribution of verbiage, documentation and information pertaining to medical reviews, current investigations, claims against HHS/FDA, and release of information to external organizations.

View All instances of the above noted in order by date

- Emails among Actors indicating a collaborative plan to produce a document defamatory to HHS/FDA that will be passed to Joan Kleinman, leaked to the press on Chris Van Hollen's letterhead and returned to Van Hollen's Office

View All instances of the above noted in order by date

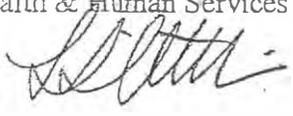
- Email among Actors indicating a collaborative plan to modify document(s) to reflect only inconsistencies and remove any speculative information.

View All instances of the above noted in order by date

MEMORANDUM

March 23, 2009

To: Leslie W. Hollie  
Supervisory Special Agent  
Office of Investigations  
Office of Inspector General  
Department of Health & Human Services

From: Les Weinstein   
Ombudsman  
Center for Devices and Radiological Health (CDRH)  
Food & Drug Administration  
Department of Health & Human Services

As you requested, enclosed are documents related to the Radiological Devices Branch and the current allegations.

Please contact me if you need any additional information.

Thank you.

HOGAN &  
HARTSON

CONFIDENTIAL FDA CDRH DMC  
JAN 13 2009

Hogan & Hartson LLP  
Columbia Square  
555 Thirteenth Street, NW  
Washington, DC 20004

www.hhlaw.com

John J. Smith, M.D., J.D.  
Partner

January 13, 2009

Received

**BY HAND DELIVERY**

PMA Document Mail Center (HFZ-401)  
Center for Devices and Radiological Health  
Office of Device Evaluation  
Food and Drug Administration  
9200 Corporate Boulevard  
Rockville, MD 20850

**Re: Possible Disclosure of Confidential iCAD, Inc., PMA Application Information  
(P010038)**

Attn: Les S. Weinstein (HFZ-5)

Dear Mr. Weinstein:

On behalf of our client, iCAD, Inc. ("iCAD" or "the company"), we are writing to provide the U.S. Food and Drug Administration ("FDA" or the "agency") with the company's letter describing possible disclosure of confidential information contained within the company's PMA application.

Should you have any questions regarding this enclosed letter, please contact me at the number above.

Sincerely,



John J. Smith, M.D., J.D.

Enclosures

**Shuren, Jeff**

**From:** Weinstein, Les S  
**Sent:** Friday, October 23, 2009 6:06 PM  
**To:** [REDACTED]  
**Cc:** Shuren, Jeff  
**Subject:** Unauthorized Disclosures

**Attachments:** Document.pdf; [REDACTED] audit.xls; NYT Jan 13 2009.pdf; [REDACTED] – clinical cardiology review  
 [REDACTED] March 26 2008.doc; Document.pdf; Document.pdf

Mr. Hollie—As you had suggested during our phone conversation yesterday, I am sending you this email regarding a third (# 1 below) unauthorized and inappropriate disclosure of information to the press in, or from, internal FDA documents regarding the review of marketing applications submitted to the Office of Device Evaluation (ODE) in FDA's Center for Devices and Radiological Health (CDRH). FDA is referring this to OIG for an investigation into this disclosure in addition to the other two disclosures (#2 and #3 below) we previously referred to OIG earlier this year.

1. On October 1, 2009, Dr. Jeff Shuren, Acting Center Director; Dr. Bram Zuckerman, Director of the Division of Cardiovascular Devices (DCD); Mathew Hillebrenner, a Branch Chief in DCD; and Timothy Ulatowski, Director of the Office of Compliance, participated in a Wall Street Journal telephone interview with reporter Alicia Mundy regarding the Edwards dETlogix annuloplasty ring ((510(k) number [REDACTED])). To their surprise Ms. Mundy was able to quote from the 510(k) reviewer's memo on [REDACTED] which is attached. The memo was completed by the lead reviewer, [REDACTED] on April 9, 2009. The 510(k) has since been cleared for marketing. It is on IMAGE (an electronic imaging system for CDRH documents). Dr. Zuckerman believes that someone from CDRH accessed IMAGE (which anyone in CDRH can do) and sent this document out. Reviewer memos are disclosable under FOIA but only after they have been officially requested and appropriately redacted. The CDRH FOIA office informed me that this memo has not been requested or released via FOIA, and that it contains trade secret (TSI) and confidential commercial information (CCI) that is not disclosable. The following memo has portions marked in pink on pages 2, 10, 11, 14, 18 and 19 indicating TSI (trade secret information) and CCI (confidential commercial information).



Document.pdf (5 MB)

To get a list of people who electronically accessed the memo, we asked our IT staff to search IMAGE audit information from the date of the memo (April 9) up to and including the date of the interview with Ms. Mundy (October 1). The following list shows that four people accessed the 25-page document indicated by the color green in column E. (The color yellow indicates a related 2-page document that is fully disclosable; I am not attaching this document.)



[REDACTED] audit.xls  
 (20 KB)

For further information please contact me or Dr. Zuckerman.

2. AngioCT device (K071871) – [REDACTED] (DCD) wrote the attached consult review memo on [REDACTED] to [REDACTED] and Dr. Robert Smith, both from the Radiological Devices Branch (RDB) in the Division of Reproductive, Abdominal, and Radiological Devices (DRARD). The memo is dated March 26, 2008. Dr. [REDACTED] was made aware of the release of this memo when it appeared in the attached New York Times article on January 13, 2009. Please let me know if OIG needs any information in addition to what FDA has already sent.



NYT Jan 13  
2009.pdf (36 KB)



██████████ -- clinical  
cardiology...

3. iCAD appealed their PMA, P010038/S12, for the SecondLook Digital product for mammography: Gardiner Harris (New York Times) spoke with iCAD on January 9, 2009. When iCAD asked the source of his information, he said it was "from internal FDA documents" and that "they were sent by scientific officers of the FDA." This product is regulated by RDB in DRARD. Please see attached correspondence to me from iCAD and their lawyer, ██████████ of Hogan and Hartson. Please let me know if OIG needs any information in addition to what FDA has already sent.



Document.pdf (1  
MB)



Document.pdf (2  
MB)

You mentioned that you would forward this email to ██████████ who now has the lead for the overall investigation into the allegations from the Radiological Devices Branch, and ██████████ who has the lead for the related investigation into the disclosure of proprietary information. Please have them call me to apprise me of the current status of these investigations. Thank you very much,

---

I wish you well in your new assignment.

Les Weinstein  
Ombudsman  
Office of the Center Director  
Center for Devices and Radiological Health  
Food and Drug Administration  
W.O. Bldg. 66 ██████████  
10903 NH Ave.  
Silver Spring MD 20993





DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General  
Office of Investigations  
Special Investigations Branch  
Washington, D.C. 20201

MAY 18 2010

Mr. Mark McCormack,  
Special Agent in Charge  
U.S. Department of Health and Human Services  
Food and Drug Administration  
Office of Criminal Investigations  
Office of Internal Affairs  
1 Church Street, [REDACTED]  
Rockville, MD 20850

RE: Case Name: Unauthorized Disclosure of Information  
OI File #: H100001413

SAC McCormack:

The U.S. Department of Health and Human Services (HHS), Office of Inspector General (OIG), Office of Investigations (OI), Special Investigations Branch (SIB), is in receipt of your referral (OIA File #: 2010-OIA-970-073). At this time, based on the information provided, OIG/OI/SIB will be taking no action. The referral lacks any evidence of criminal conduct on the part of any HHS employee. Additionally, 5 U.S.C. § 1213, identifies that disclosures, such as the ones alleged, when they relate to matters of public safety may be made to the media and Congress as long as the material released is not specifically prohibited by law and protected by Executive Order or National Security Classification.

The OIG is appreciative of your support in its overall mission. Thank you for contacting the OIG on this matter. Should you have any questions, or need any additional information, please feel free to contact me at [REDACTED]

Respectfully,

Scott A. Vantrease  
Assistant Special Agent in Charge  
Special Investigations Branch



## DEPARTMENT OF HEALTH &amp; HUMAN SERVICES

Food and Drug Administration  
10903 New Hampshire Avenue  
Silver Spring, MD 20993-0002

June 28, 2010

Daniel Levinson, Inspector General  
U.S. Department of Health and Human Services  
Office of Inspector General  
Washington, DC 20201

RE: Case Number: Unauthorized Disclosure of Information  
OI File#: H100001413

Dear Mr. Levinson:

We are in receipt of the letter dated May 18, 2010, from Scott A. Vantrease, Assistant Special Agent in Charge, Special Investigations Branch. Thank you for your quick response to our request for an investigation. However, we are now making a new request for an OIG investigation. We have obtained new information confirming the existence of information disclosures that undermine the integrity and mission of the FDA and, we believe, may be prohibited by law. Furthermore, these disclosures may be ongoing. We request that the OIG promptly review this new information.

On May 17, 2010, the FDA Office of Internal Affairs (OIA), Mark McCormack, Special Agent in Charge, requested that the OIG review what the FDA determined to be an inappropriate disclosure of confidential commercial information in the potential release of information related to a pending GE Healthcare application. The OIG determined based on the information presented at the time that the referral lacked evidence of criminal conduct and declined to take action.

We now have additional evidence, based on an internal investigation, that several employees may have engaged in the unlawful disclosure of confidential commercial information. We undertook this internal investigation because we had reason to believe that an employee may have been responsible for leaking confidential commercial information. Based on our reasonable suspicion, OIA authorized the Office of Information Management (OIM) to institute real-time monitoring of his FDA computer, using narrowly tailored search criteria relating to device cases to which he was assigned.

Our monitoring, which is ongoing, produced documents suggesting that employees are engaged in the inappropriate, and likely illegal, disclosure of nonpublic information. These documents are being forwarded to your secure IT portal. Specifically, they show that the employee at issue and other employees have recently disclosed nonpublic information to at least one former FDA employee relating to full field digital mammography (FFDM), spine analysis software, and infant enteral feeding tube device

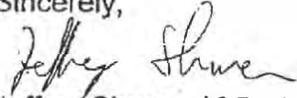
application files. In the case of the FFDM device submission, the employees sharing and discussing the company-confidential information with the unauthorized recipient were officially assigned to review these files, but the unauthorized recipient lacked any prior history with these files or specific expertise that might justify seeking his input (notwithstanding that such disclosure may be illegal). In another case, employees assigned to the review of spine analysis software shared with the former employee information about the content and ongoing review of that file. In a third case, the employees shared with the former employee information from infant enteral feeding tube, accessories, and tube extension set files that they were not officially assigned to review, and there was no apparent justification for disclosing or discussing the files with the unauthorized recipient. We have also discovered emails that the employee in question sent to unauthorized recipients which appear to have attachments likely containing confidential commercial information, but we have not yet confirmed that we have all the attachments themselves. For example, the employee sent an email to the former employee asking for comments on a hemodialysis device file.

Notably, the OIA-authorized monitoring by OIM has not involved analysis of past periods, during which leaks relating to the GE Healthcare device application or other matters may have occurred; a retrospective analysis would actually require a review of the contents of the subject employee's government-issued computer and the government-issued computer(s) of other identified employee(s), which would be facilitated by the opening of a formal investigation. We have also determined that nonpublic information from multiple device application files was improperly downloaded from the employee's FDA computer to a non-FDA computer and to portable storage devices; further investigation may determine that these downloads resulted in additional disclosures of confidential commercial information.

We request that you review the attached communications to determine whether this would warrant opening an investigation to determine whether one or more employees may have engaged in unlawful conduct. We believe that the emails and attached documents represent disclosures that may be prohibited by law. Among other things, the federal Food, Drug, and Cosmetic Act (the Act) prohibits anyone "revealing, other than to the Secretary or officers or employees of the Department, or to the courts when relevant..., any information acquired under the" FDA's authority to review and approve applications for devices and other products. 21 U.S.C. § 331(j). Moreover, the Act prohibits the disclosure of confidential commercial information without the written consent of the sponsor who submitted the information. 21 U.S.C. § 331(y). In the case of a device not on the market, for which the intent to market the device has not been disclosed, and that has been submitted to the FDA for premarket approval or premarket notification review, FDA generally may not disclose the existence of the premarket submission. 21 C.F.R. §§ 807.95 & 814.9. More generally, any federal employee who discloses confidential trade secret information is subject to a fine or imprisonment. See also 45 C.F.R. § 73.735-307(3) (prohibiting FDA employees from disclosing information obtained in confidence, in accordance with applicable federal laws).

We are particularly concerned that the continued release of confidential information has compromised or will compromise the integrity of the ongoing premarket review of the subject device applications. Therefore, we request that the OIG immediately review this new information and open an investigation.

Sincerely,



Jeffrey Shuren, M.D., J.D.  
Director, Center for Devices  
and Radiological Health  
Food and Drug Administration

Attachments



U.S. Department of Justice

Criminal Division

---

Washington, D.C. 20530

NOV - 3 2010

Mr. David Mehring  
Special Agent  
Office of the Inspector General  
Department of Health and Human Services  
330 Independence Avenue SW  
[REDACTED]  
Washington, DC 20201

Re: Dr. Robert Smith

Dear Mr. Mehring:

The Public Integrity Section has reviewed the above-referenced matter in which there were alleged violations of Title 18, United States Code, Section 1905, perpetrated by Dr. Robert Smith and other employees of the Food and Drug Administration's Center for Devices and Radiological Health. After reviewing this matter, we have decided to decline prosecution. We understand that your office concurs with this decision.

If you have any questions regarding this matter, please contact me at [REDACTED].  
Thank you for your cooperation in this matter.

Sincerely,

Jack Smith  
Chief  
Public Integrity Section



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General  
Office of Investigations  
Special Investigations Branch  
330 Independence Avenue, S.W.  
Washington, DC 20201

NOV 15 2010

TO: Dr. Jeffrey Shuren  
Director  
Center for Devices and Radiological Health  
Food and Drug Administration

FROM: Scott A. Vantrease   
Assistant Special Agent in Charge  
Special Investigations Branch

SUBJECT: Closure of Investigation Concerning Paul Hardy, Dr. Ewa Czerska, and Dr. Robert Smith  
OI File Number: H-10-00248-3

On July 31, 2010, the Office of Investigations (OI), Special Investigations Branch (SIB), opened an investigation regarding your complaint referral that alleged several employees within the Food and Drug Administration (FDA), Center for Devices and Radiological Health (CDRH), had disclosed confidential information, as such undermining the integrity and mission of the FDA. Investigators with OI/SIB reviewed the complaint, met with several FDA staff, including the FDA Assistant Commissioner for Management to obtain additional information about the alleged misconduct.

After completing a review, OI/SIB investigators discussed the alleged misconduct, along with the evidence identified during FDA's internal investigation, with prosecutors from the U.S. Department of Justice. The prosecutors performed a thorough review of the matter, and declined prosecution. At this time, OI/SIB is closing its investigation of this matter. Your office indicated it had developed sufficient evidence to address the alleged misconduct through administrative processes, and as such, no further action will be taken by OIG.

If you have any questions or require additional information, please contact SIB, ASAC, Scott A. Vantrease at 



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

June 20, 2012

MEMORANDUM FOR CHIEF INFORMATION OFFICERS AND GENERAL COUNSELS

FROM:

Steven VanRoekel  
Federal Chief Information Officer

A handwritten signature in black ink, appearing to read "S. VanRoekel".

Boris Bershteyn  
General Counsel

A handwritten signature in black ink, appearing to read "B. Bershteyn".

SUBJECT:

Office of Special Counsel Memorandum on Agency Monitoring Policies and Confidential Whistleblower Disclosures

The attached memorandum from the Office of Special Counsel (OSC) identifies certain legal restrictions and guidelines that executive departments and agencies should consider when evaluating their policies and practices regarding monitoring of employee electronic mail and other communications. Although lawful agency monitoring of employee communications serves legitimate purposes, Federal law also protects the ability of workers to exercise their legal rights to disclose wrongdoing without fear of retaliation, which is essential to good government.

We strongly urge you to carefully review the attached OSC memorandum when evaluating your agency's monitoring policies and practices, and to take appropriate steps to ensure that those policies and practices do not interfere with or chill employees' use of appropriate channels to disclose wrongdoing.



U.S. OFFICE OF SPECIAL COUNSEL  
1730 M Street, N.W., Suite [REDACTED]  
Washington, D.C. 20036-4505  
202-[REDACTED]

June 20, 2012

MEMORANDUM FOR EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Special Counsel Carolyn N. Lerner *Carolyn Lerner*  
U.S. Office of Special Counsel

SUBJECT: Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General

This memorandum identifies certain legal restrictions and guidelines that agencies should consider when evaluating their policies and practices regarding monitoring of employee electronic mail and other communications. Although lawful agency monitoring of employee communications serves legitimate purposes, Federal law also protects the ability of workers to exercise their legal rights to disclose wrongdoing without fear of retaliation, which is essential to good government. Indeed, Federal employees are required to disclose waste, fraud, abuse, and corruption to appropriate authorities<sup>1</sup> and are expected to maintain concern for the public interest,<sup>2</sup> which may include disclosing wrongdoing.

We strongly urge executive departments and agencies (agencies) to evaluate their monitoring policies and practices, and take measures to ensure that these policies and practices do not interfere with or chill employees from using appropriate channels to disclose wrongdoing. The following legal restrictions and guidelines should be considered as part of this evaluation.

**Legal Framework**

Federal law generally prohibits adverse personnel actions against a Federal employee because of an employee's disclosure of information that the employee reasonably believes evidences a violation of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.<sup>3</sup> Subject to certain exceptions, Federal law also protects the identity of an employee who makes

---

<sup>1</sup> See Ethics Principle No. 11, 5 C.F.R. § 2635.101(b)(11).

<sup>2</sup> See Merit Principle No. 4, 5 U.S.C. § 2301(b)(4).

<sup>3</sup> See 5 U.S.C. § 2302(b)(8).

such a protected disclosure to the Office of Special Counsel (OSC) or an agency Inspector General (IG).<sup>4</sup>

### **Guidelines**

In light of this legal framework, agency monitoring specifically designed to target protected disclosures to the OSC and IGs is highly problematic. Such targeting undermines the ability of employees to make confidential disclosures. Moreover, deliberate targeting by an employing agency of an employee's submission (or draft submissions) to the OSC or an IG, or deliberate monitoring of communications between the employee and the OSC or IG in response to such a submission by the employee, could lead to a determination that the agency has retaliated against the employee for making a protected disclosure. The same risk is presented by an employing agency's deliberate targeting of an employee's emails or computer files for monitoring simply because the employee made a protected disclosure.

### **Summary**

In sum, we strongly recommend that agencies review existing monitoring policies and practices to ensure that they are consistent with both the law and Congress's intent to provide a secure channel for protected disclosures.

---

<sup>4</sup> See 5 U.S.C. § 1213(h) (prohibiting the Special Counsel from disclosing the identity of a whistleblower without the individual's consent unless disclosure becomes necessary due to an imminent danger to public health or safety or imminent violation of any criminal law); 5 U.S.C. App. § 7(b) (prohibiting IGs from disclosing the identity of a whistleblower without the whistleblower's consent unless an IG determines such disclosure is unavoidable during the course of an investigation).



U.S. Office of Special Counsel  
1730 M Street, N.W., Suite [REDACTED]  
Washington, D.C. 20036-4505

## Office of Special Counsel Broadens Investigation into FDA's Surveillance of Employees' E-mail

---

**FOR IMMEDIATE RELEASE**

**CONTACT: Ann O'Hanlon, 202-** [REDACTED] [REDACTED]

The Office of Special Counsel (OSC) has broadened the scope of an existing investigation into the surveillance of employees' emails by the Food and Drug Administration (FDA). FDA acknowledged that it monitored emails at the Center for Devices and Radiological Health to congressional investigators and the OSC after the employees reported coercion to approve unsafe or harmful medical devices.

Recently, OSC received new and troubling allegations of retaliatory surveillance of OSC communications and other acts of retaliation against the whistleblowers, including FDA attempts to initiate criminal prosecution of the whistleblowers. We are reviewing these additional allegations and information from Congress and will take appropriate action.

Relying on documents obtained through FOIA, the whistleblowers allege that the agency reviewed disclosures intended specifically for OSC, and that the agency also monitored the communications of employees who were suspected of blowing the whistle on FDA's approval of unsafe medical devices. These disclosures indicated repeated attempts by employees to warn the public that the devices were not safe and should not have received FDA approval.

Under the Whistleblower Protection Act, federal employees are authorized to provide any information to OSC, including confidential business information, in order to disclose government waste, fraud, abuse, gross mismanagement or health and safety issues. In establishing the OSC, Congress intended to provide a secure channel for disclosures, and whistleblowers are entitled to keep their disclosures to OSC confidential. Even where an agency has a legitimate basis to monitor an employee's email or has a warning regarding email monitoring, that basis or warning does not trump the employees' right to confidentially blow the whistle to OSC or Congress.

"Monitoring employee emails with OSC or Congress could dissuade employees from making important disclosures," said Special Counsel Carolyn Lerner. "Monitoring communications with OSC is unacceptable. We encourage other agencies to review their policies to ensure that they are not monitoring or otherwise impeding employee disclosures to OSC or Congress."

\*\*\*

*The U.S. Office of Special Counsel (OSC) is an independent federal investigative and prosecutorial agency. Our basic authorities come from four federal statutes: the Civil Service Reform Act, the Whistleblower Protection Act, the Hatch Act, and the Uniformed Services Employment & Reemployment Rights Act (USERRA). OSC's primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices, especially reprisal for whistleblowing. For more information, please visit our website at [www.osc.gov](http://www.osc.gov).*



DEPARTMENT OF HEALTH AND HUMAN SERVICES

---

Food and Drug Administration  
Center for Devices and Radiological Health  
9200 Corporate Boulevard  
Rockville, MD 20850

January 7, 2009

John D. Podesta  
Presidential Transition Team  
Washington, DC 20270

Dear Mr. Podesta:

We, physicians and scientists of the U.S. Food and Drug Administration (FDA), fully support the agenda of President Obama to “challenge the status quo in Washington and to bring about the kind of change America needs.”<sup>1</sup> America urgently needs change at FDA because FDA is fundamentally broken, failing to fulfill its mission, and because re-establishing a proper and effectively functioning FDA is vital to the physical and economic health of the nation. As stated in the November 2007 FDA Science Board Report<sup>2</sup> entitled *FDA Science and Mission at Risk*: “A strong FDA is crucial for the health of our country. The benefits of a robust, progressive Agency are enormous; the risks of a debilitated, under-performing organization are incalculable. The FDA constitutes a critical component of our nation’s healthcare delivery and public health system. The FDA, as much as any public or private sector institution in our country, touches the lives, health and well-being of all Americans. ... The FDA is also central to the economic health of the nation, regulating approximately \$1 trillion in consumer products or 25 cents of every consumer dollar expended in this country annually. ... The importance of the FDA in the nation’s security is similarly profound. ... Thus, the nation is at risk if FDA science is at risk.”

The purpose of this letter is to inform you that the scientific review process for medical devices at FDA has been corrupted and distorted by current FDA managers, thereby placing the American people at risk. Through this letter and your action, we hope that future FDA employees will not experience the same frustration and anxiety that we have experienced for more than a year at the hands of FDA managers because we are committed to public integrity and were willing to speak out. Currently, there is an atmosphere at FDA in which the honest employee fears the dishonest employee, and not the other way around. Disturbingly, the atmosphere does not yet exist at FDA where honest employees committed to integrity and the FDA mission can act without fear of reprisal. This letter provides an inside view of the severely broken science, regulation and administration at the Center for Devices and Radiological Health (CDRH) that recently forced FDA physicians and scientists to seek direct intervention from the U.S. Congress.<sup>3</sup> This letter also provides elements of reform that are necessary to begin real change at FDA from the “bottom up.”

Since May 2008,<sup>4</sup> the FDA Commissioner has been provided with irrefutable evidence that managers at CDRH have placed the nation at risk by corrupting and distorting the scientific evaluation of medical devices, and by interfering with our responsibility to ensure the safety and effectiveness of medical devices before they are used on the American public. Before a medical device can be cleared or approved by FDA, the law requires<sup>5</sup> that safety and effectiveness is determined based on “valid scientific evidence ... from which it can fairly and responsibly be

concluded by qualified experts that there is reasonable assurance of the safety and effectiveness of the device.” Managers at CDRH have ignored the law and ordered physicians and scientists to assess medical devices employing unsound evaluation methods, and to accept non-scientific, nor clinically validated, safety and effectiveness evidence and conclusions, as the basis of device clearance and approval. Managers with incompatible, discordant, and irrelevant scientific and clinical expertise in devices for which they have the full authority to make final regulatory decisions, have ignored serious safety and effectiveness concerns of FDA experts. Managers have ordered, intimidated, and coerced FDA experts to modify scientific evaluations, conclusions and recommendations in violation of the laws, rules and regulations and to accept clinical and technical data that is not scientifically valid nor obtained in accordance with legal requirements, such as obtaining proper informed consent from human subjects. These same managers have knowingly tried to avoid transparency and accountability by failing to properly document the basis of their non-scientific decisions in administrative records. As examples of wrongdoing, the Director of the Office of Device Evaluation (ODE) has gone so far as to:

- Order physicians and scientists to ignore FDA Guidance documents;
- Knowingly allow her subordinates to issue written threats of disciplinary action if physicians and scientists failed to change their scientific opinions and recommendations to conform to those of management;
- Issue illegal internal documents that do not conform to the requirements of Good Guidance Practices,<sup>6</sup> are not publicly available, and, if followed, would circumvent science and legal regulatory requirements;
- Fail to properly document significant decisions in the administrative files;<sup>7</sup>
- Make, and allow, false statements in FDA documents;
- Allow manufacturers to market devices that have never been approved by FDA;
- Remove Black Box warnings recommended by FDA experts;
- Bypass FDA experts and fail to properly label devices; and
- Exclude FDA experts from participating in Panel Meetings<sup>8</sup> because manufacturers “expressed concerns that [FDA experts] are biased.”

For seven months, Dr. von Eschenbach and his Assistant Commissioner for Accountability and Integrity (Mr. Bill McConagha) have conducted a sham investigation resulting in absolutely nothing; no one was held accountable, no appropriate or effective actions have been taken, and the same managers who engaged in the wrongdoing remain in place and have been rewarded and promoted. Dr. von Eschenbach and Mr. McConagha failed to take appropriate or effective actions while the physicians and scientists who had the courage and patriotism to speak out, and who refused to comply with FDA management wrongdoing, have suffered severe and ongoing retaliation.<sup>9</sup> The failure of Dr. von Eschenbach and Mr. McConagha to take appropriate or effective actions has made them complicit in the wrongdoing,<sup>10</sup> has harmed the reputations and lives of individual employees, and has unnecessarily placed the American public at risk.

In October 2008, the U.S. Congress was provided with the same evidence of wrongdoing that was given to the Commissioner. After Congress examined the evidence, the U.S. House of Representatives Committee on Energy and Commerce sent a letter to the FDA Commissioner dated November 17, 2008,<sup>11</sup> stating that they had “received compelling evidence of serious wrongdoing ... and well-documented allegations ... from a large group of scientists and physicians ... who report misconduct within CDRH that represents an unwarranted risk to public health and a silent danger that may only be recognized after many years ... and that physicians and scientists

within CDRH who objected [to the misconduct]... have been subject to reprisals.”

Unfortunately, the preceding facts are only the latest examples of shocking managerial corruption, wrongdoing and retaliation at CDRH. Back in February 2002, a biomedical engineer at CDRH reported serious managerial misconduct to the current Director of ODE and ultimately filed an EEOC lawsuit in September 2004. After six long stressful years of hardship and litigation, a Judge issued a forty-two page *Decision and Findings of Fact*<sup>12</sup> concluding that: “the Agency promoted a hostile working environment ... permeated with derogatory comments and adverse employment actions” ... the Agency “failed to exercise any reasonable care to prevent and correct promptly the harassing behavior” ... the actions toward the engineer were “unconscionable” and “occurred openly within the FDA, unchecked, for over four years” ... that “FDA managers were aware and failed to take appropriate or effective corrective actions; but rather, demonstrated a systemic disregard for federal regulations as well as the FDA's own policies.” The Judge further concluded: “supervisors [including the current Director of ODE] knew or should have known of the hostile work environment, but neither the supervisors nor the Agency did anything to correct the situation or prevent further discrimination” ... and “failed to exercise any reasonable care to prevent or correct the hostility of [managers] towards the Complainant.” Shockingly, the current Director of ODE herself testified in court that she was aware of the “hostile work environment” but “did not want to get involved,” thereby corroborating her complicity in the corruption and retaliation against this employee. These independent facts confirm the longstanding pandemic corruption that cries out for new leadership at FDA from the bottom up.

We are confident that new leadership from the bottom up will be a top priority of Mr. Daschle as the new Secretary of the Department of Health and Human Services (HHS). As Mr. Daschle has recognized,<sup>13</sup> the integrity of the FDA scientific review and decision-making process, where scientific experts make evaluations and recommendations, must be evidence-based and independent, insulated from improper influences. As a matter of fact, Mr. Daschle points to the 1998 FDA approval of mammography computer-aided detection (CAD) devices<sup>14</sup> as an example of a breakdown of the independent scientific review and decision-making process. These CAD devices were supposed to improve breast cancer detection on mammograms. As Mr. Daschle recognized, post-approval scientific publications revealed that actual clinical performance of these CAD devices did not improve breast cancer detection<sup>15</sup> and they were associated with increased patient recalls and unnecessary breast biopsies.<sup>16</sup> We note that the Agency knowingly approved these devices in 1998 even though there was no clinical evidence of improved cancer detection and, furthermore, the device was never tested in accordance with its intended use— one of the principal required elements for device approval.<sup>17</sup> Astoundingly, the approval was based on pseudo-science that consisted of unsubstantiated estimates of potential benefit using flawed testing. Use of these devices is a major public health issue as approximately 40 million mammograms are performed every year in the U.S.<sup>18</sup> Furthermore, as a failure of FDA post-approval monitoring, the FDA never carried out any post-marketing assessment or re-evaluation of the clinical performance of these devices, ignoring accumulating clinical evidence provided by independent research publications revealing that these devices were ineffective and potentially harmful when used in clinical practice.

FDA managers continue to fail to apply even the most fundamental scientific and legal requirements for the approval of these, and so many other, devices. These failures constitute a clear and silent danger to the American public. Since 2006, FDA physicians and scientists have recommended five times not to approve mammography CAD devices without valid scientific and clinical evidence of safety and effectiveness. Manufacturers of these devices have repeatedly

failed to provide valid scientific and clinical evidence demonstrating safety and effectiveness of these devices in accordance with the intended use as required by the law. These matters were the subject of a Radiological Devices Panel meeting in March 2008<sup>19</sup> at which independent outside experts ratified all of the scientific, clinical, and regulatory points of the FDA experts required for proper assessment of the safety and effectiveness of these devices. Despite this, in April of 2008, the Director of ODE ignored the recommendations of all of the experts and approved these devices without any scientific, clinical or legal justification. Although unknown to Mr. Daschle and the American public, the Director of ODE and her subordinates committed the most outrageous misconduct by ordering, coercing, and intimidating FDA physicians and scientists to recommend approval, and then retaliating when the physicians and scientists refused to go along. This, and similar management actions with other devices, compelled us to write the FDA Commissioner in May 2008 and, because he utterly failed to take appropriate or effective actions, we later informed the U.S. Congress in October 2008.

We, physicians and scientists at FDA, seek your immediate attention for change and reform at FDA. To bring real change and reform to FDA, it is absolutely necessary that Congress pass, and the President<sup>20</sup> sign, new legislation providing the strongest possible protections for all government employees,<sup>21</sup> especially physicians and scientists, who speak out about wrongdoing and corruption that interferes with their mission and responsibility to the American public. We desperately need honesty without fear of retaliation for our evaluations and recommendations on medical devices, as well as accountability and transparency, to become the law and thus the foundation of the FDA mission and workplace. We totally agree with the following statement of President Obama:<sup>22</sup> “Often the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out. Such acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars, should be encouraged rather than stifled. We need to empower federal employees as watchdogs of wrongdoing and partners in performance. Barack Obama will strengthen whistleblower laws to protect federal workers who expose waste, fraud, and abuse of authority in government. Obama will ensure that ... whistleblowers have full access to courts and due process.”

As President Obama has emphasized, he intends to govern the nation and to bring about change from the bottom up. We believe that, as applied to FDA, this means a complete restructuring of the evaluation and approval process such that it is driven by science and carried out by clinical and scientific experts in their corresponding areas of expertise who are charged with review of regulatory submissions in accordance with the laws, rules and regulations. It is necessary that FDA expert physicians and scientists approve final regulatory determinations of safety and effectiveness, rather than multiple layers of managers who are not qualified experts and who often ignore scientific evidence and the law. President Obama has also emphasized the need for complete transparency in government. His Transparency Policy<sup>23</sup> should be mandatory for all FDA regulatory decisions and associated documentation. The long-standing FDA practice of secret meetings and secret communications between FDA managers and regulated industry must be strictly prohibited. Complete transparency in the regulatory decision-making process would serve as a deterrent to wrongdoing and an incentive for excellence.

FDA also requires major renovation of the organizational structure of the various Centers and Offices to restore internal checks and balances that proactively prevent corruption and manipulation of facts, science, and data. At present, FDA is plagued by a heavy-layered top-down organizational structure that concentrates far too much power in isolated Offices run by entrenched managers where cronyism is paramount. We recommend that the Office of Device Evaluation be

dismantled and split into multiple Offices, each headed by a physician or scientist with strong leadership credentials and extensive clinical and technical expertise in the specific devices they regulate. These leadership positions should be rotated on a regular basis. Furthermore, the current system of employee performance evaluation must be eliminated because it is used as an instrument of extortion by management and to terrorize employees who would otherwise serve as “watchdogs of wrongdoing and partners in performance.”<sup>24</sup> The performance of FDA physicians and scientists must be based on an independent peer review process where extramural experts review the quality of the scientific content of their regulatory work.

We strongly support the sentiments expressed in a recent letter from Congressman Bart Stupak<sup>25</sup> urging complete change in FDA's current leadership. At CDRH, such change can be implemented immediately by removing and punishing all managers who have participated in, fostered or tolerated the well-documented corruption and wrongdoing. All improper management actions, including improper adverse personnel actions, and clearance/approval of medical devices that were not made in accordance with the laws, rules and regulations, must be reversed. Such swift and decisive action of transparency and accountability will send a strong message FDA-wide that wrongdoing will no longer be tolerated. In order to have a truly fresh start, we recommend that the new Commissioner request resignations from management positions by all current managers within CDRH, and use a competitive merit-based process to re-fill all management positions.

The FDA mission is not limited to pre-market evaluation of safety and effectiveness. FDA is also responsible for the total product life cycle including actual clinical performance.<sup>26</sup> FDA must not engage in a fire-fighting regulatory posture after medical products are introduced into clinical practice and used on patients.<sup>27</sup> FDA must pursue a culture of proactive regulatory science and remain vigilant in monitoring clinical performance of devices. For FDA to fully accomplish its post-marketing responsibilities there must be complete coordination between FDA and all HHS health-related agencies and institutes.<sup>28</sup> This will provide FDA with the necessary critical scientific capability and capacity<sup>29</sup> to achieve its post-marketing oversight. In turn, FDA will be able to provide the American public and all health care decision makers with objective and scientifically rigorous assessments that synthesize available evidence on diagnosis, treatment and prevention of disease. Ultimately, this will result in a lower health care burden on our society.

In a time of transition, with the country facing an economic crisis with potential devastating consequences to the American people, we strongly believe that change and reform at FDA must be a top priority because FDA is central to the physical and economic health of the nation and because it can play a central role in reducing the future healthcare burden and avoiding public health catastrophes.<sup>30</sup> We sincerely hope that, together, we can establish a culture of science, honesty, transparency and integrity at FDA to serve as the genesis of reform for the entire American health care system.

Sincerely,

Cc: Senator Tom Daschle, HHS Secretary-Designate  
Dr. Joshua Sharfstein, HHS Transition Team  
Congressman John Dingell  
Congressman Henry Waxman  
Congressman Bart Stupak  
Congressman Chris Van Hollen  
Senator Edward Kennedy  
Senator Michael Enzi  
Senator Barbara Mikulski  
Senator Max Baucus  
Senator Chuck Grassley

<sup>1</sup> See <http://change.gov/agenda/>

<sup>2</sup> See [http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b\\_02\\_00\\_index.html](http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b_02_00_index.html)

<sup>3</sup> See <http://energycommerce.house.gov/images/stories/Documents/PDF/Newsroom/110-ltr-101408.CDRHscientists.pdf>;  
<http://energycommerce.house.gov/images/stories/Documents/PDF/Newsroom/110-ltr-111708.vonEschenbach.CDRH.pdf>

<sup>4</sup> See letter to Dr. Andrew von Eschenbach dated May 30, 2008; See also documentary evidence provided to Dr. von Eschenbach and Mr. Bill McConagha beginning in June 2008.

<sup>5</sup> See 21 CFR 860.7.

<sup>6</sup> See 21 CFR 10.115.

<sup>7</sup> See 21 CFR 10.70.

<sup>8</sup> See <http://www.citizen.org/publications/release.cfm?ID=7620>

<sup>9</sup> See letter to Mr. Bill McConagha dated October 20, 2008.

<sup>10</sup> See letter to Dr. Andrew von Eschenbach dated September 29, 2008.

<sup>11</sup> See <http://energycommerce.house.gov/images/stories/Documents/PDF/Newsroom/110-ltr-111708.vonEschenbach.CDRH.pdf>

<sup>12</sup> EEOC No. 531-2006-00114X.

<sup>13</sup> See e.g., pages 116-128 and 169-180 of *CRITICAL--WHAT WE CAN DO ABOUT THE HEALTH-CARE CRISIS*, by Senator Tom Daschle, Thomas Dunne Books, New York, 2008.

<sup>14</sup> Id. at page 121.

<sup>15</sup> See <http://www.fda.gov/ohrms/dockets/ac/08/briefing/2008-4349b1-01%20FDA%20Radiological%20Devices%20Panel%20Meeting%20Introduct.pdf> at pages 52-56.

<sup>16</sup> See Id. at pages 42 and 52-56.

<sup>17</sup> See 21 CFR 860.7.

<sup>18</sup> See <http://www.fda.gov/CDRH/MAMMOGRAPHY/scorecard-statistics.html>

<sup>19</sup> See <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfAdvisory/details.cfm?mte=694>

<sup>20</sup> See [http://www.whistleblowers.org/index.php?option=com\\_content&task=view&id=695&Itemid=100](http://www.whistleblowers.org/index.php?option=com_content&task=view&id=695&Itemid=100)

<sup>21</sup> See the December 2008 Report from the Union of Concerned Scientists, *Federal Science and the Public Good--Securing the Integrity of Science in Policymaking*, available at

[http://www.ucsusa.org/assets/documents/scientific\\_integrity/Federal-Science-and-the-Public-Good-12-08-Update.pdf](http://www.ucsusa.org/assets/documents/scientific_integrity/Federal-Science-and-the-Public-Good-12-08-Update.pdf).

<sup>22</sup> See [http://change.gov/agenda/ethics\\_agenda/](http://change.gov/agenda/ethics_agenda/)

<sup>23</sup> See [http://change.gov/page/-/open%20government/yourseatatthetable/SeatAtTheTable\\_memo.pdf](http://change.gov/page/-/open%20government/yourseatatthetable/SeatAtTheTable_memo.pdf)

<sup>24</sup> See [http://change.gov/agenda/ethics\\_agenda/](http://change.gov/agenda/ethics_agenda/)

<sup>25</sup> See <http://online.wsj.com/public/resources/documents/stupak-letter-to-obama-20081205.pdf>

<sup>26</sup> See <http://www.fda.gov/cdrh/strategic/tpic.html>

<sup>27</sup> See page 4, Section 1.2.1 at [http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b\\_02\\_01\\_FDA%20Report%20on%20Science%20and%20Technology.pdf](http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b_02_01_FDA%20Report%20on%20Science%20and%20Technology.pdf)

<sup>28</sup> See <http://www.hhs.gov/about/orgchart/>

<sup>29</sup> See page 44, Section 3.2.4 at [http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b\\_02\\_01\\_FDA%20Report%20on%20Science%20and%20Technology.pdf](http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b_02_01_FDA%20Report%20on%20Science%20and%20Technology.pdf)

<sup>30</sup> See, e.g. National Center for Health Statistics, Health, United States, 2007, with Chartbook on Trends in the Health of Americans, available at <http://www.cdc.gov/nchs/data/has/has07.pdf>; and 2008 World Cancer Report, available at <http://www.iarc.fr/en/Publications/PDFs-online/World-Cancer-Report>

Note: We can provide all documents referenced in footnotes upon your request.

Never stop looking



January 13, 2009

Les S. Weinstein  
Ombudsman and Quality Assurance Manager  
Center for Devices and Radiological Health (HFZ-5)  
Food and Drug Administration  
9200 Corporate Boulevard  
Rockville, Maryland 20850

RE: Possible Disclosure of Confidential iCAD, Inc., PMA Application Information

Dear Mr. Weinstein,

I am writing to bring to the Food and Drug Administration's attention a possible serious breach of confidentiality concerning the Company's premarket approval applications on the part of an unknown individual or individuals at the agency. It was our intention to bring this matter to the attention of the agency's Integrity Officer but it is our understanding that the position is vacant at this time.

On Thursday, January 8, 2009, I was contacted by [REDACTED] the [REDACTED] for Fujifilm Medical Systems USA, Inc., a company with which iCAD has partnered in regard to iCAD's SecondLook® Digital Computer-aided Detection for Mammography device [REDACTED]. In our discussion, [REDACTED] related that Fuji had received a telephone call earlier that day from Gardiner Harris, an individual representing himself as a reporter from the New York Times. [REDACTED] noted that Mr. Harris was under the misimpression that "iCAD" was a Fuji device and was seeking Fuji's opinion concerning very specific questions on certain documents related to the approval of this "device" that had come into the possession of the New York Times. [REDACTED] indicated that Mr. Harris further implied that a member of Congress had intervened in this product's review process and had pressured an FDA official to support approval of the device. During the course of the conversation, it became apparent to [REDACTED] that Mr. Harris was referring to the approval of iCAD's SecondLook® device for use with Fuji's computed radiographic mammography system [REDACTED]. Accordingly, Mr. Harris was informed that iCAD was a separate corporate entity. Mr. Harris in turn indicated that he would contact iCAD regarding these documents and the SecondLook®.

98 Spa Brook Road, Suite [REDACTED] Nashua, NH 03062 USA

+1 866 280 2239 toll free [REDACTED]

[www.icadmed.com](http://www.icadmed.com)

Never stop learning



On Friday, January 9, I personally spoke with Mr. Harris by phone with Ms. Darlene Deptula-Hicks, our EVP and CFO, also present in the room during the conversation. In our discussion, Mr. Harris stated that he was in receipt of "internal FDA documents" that were sent to him by "Scientific Officers of the FDA." During the course of our conversation, Mr. Harris asked a number of questions that clearly reflected a depth of detail and knowledge that only would be known to either the Company or the FDA, and not generally available to the public. I can assure you that the Company has not disclosed this sensitive information to the New York Times, or to any other individuals or organizations outside of its business partners or attorneys, and only then with the appropriate confidentiality protections in place.

As you are aware, under 21 C.F.R. § 814.9, confidential information submitted to the agency as part of a premarket approval application or a supplement to that application cannot be released by FDA without the explicit permission of a PMA sponsor. From the discussion with Mr. Harris, I am deeply concerned that information concerning [REDACTED], and potentially other Company submissions, have been shared with the New York Times. Further, articles that have contemporaneously appeared in other media outlets suggest that the disclosure of this information may have involved organizations beyond the New York Times. I have attached a sample of these articles for your reference.

We appreciate your attention to this serious matter. Should you require any additional information, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script that reads "Ken Ferry".

Ken Ferry  
President and Chief Executive Officer

Cc: [REDACTED], M.D.  
[REDACTED], Ph.D.  
[REDACTED], M.D., J.D.

98 Spit Brook Road, Suite [REDACTED] Nashua, NH 03062 USA  
+1 856 280 2239 toll free [REDACTED]  
[www.icadmed.com](http://www.icadmed.com)

KING & SPALDING LLP

King & Spalding LLP  
1700 Pennsylvania Avenue, N.W.  
Washington, DC 20006-4705

Edward M. Basile  
Senior Partner

April 16, 2010

VIA HAND DELIVERY

Dr. Jeffery E. Shuren, Director  
Center for Devices and Radiological Health  
U.S. Food and Drug Administration  
10903 New Hampshire Avenue  
[REDACTED]  
Silver Spring, MD 20993

Dear Dr. Shuren:

I am writing on behalf of GE Healthcare, a unit of General Electric Company ("GE Healthcare"), to express its disappointment in the Center for Devices and Radiological Health ("CDRH") for disclosing to the press confidential information in GE Healthcare's premarket notification ("510(k)") submission dated November 26, 2008 and received by CDRH on December 1, 2008. On March 28, 2010, a *New York Times* article by Gardiner Harris entitled, "Scientists Say F.D.A. Ignored Radiation Warnings," revealed that "scores of internal agency documents" regarding GE Healthcare's submission were provided to the *New York Times*. See Appendix I. GE Healthcare is extremely concerned about this violation of confidentiality and respectfully requests that you conduct an internal investigation into how this information was leaked to the press. GE Healthcare also requests a meeting with you to discuss steps you plan to take going forward to ensure that breaches of confidentiality such as this one do not happen again.

While the Food and Drug Administration's ("FDA") general policy is to allow disclosure of information, specific conditions constrain when FDA, and therefore, CDRH, may disclose the existence and contents of 510(k) submissions. None of these conditions were present when CDRH disclosed information to the *New York Times*. CDRH was not permitted to publicly disclose either the existence or the contents of GE Healthcare's 510(k) submission, so in disclosing this information, CDRH breached the confidentiality of GE Healthcare's submission in violation of both federal regulations and internal agency policy.

WDC\_IMANAGE-1455066.1

I. Conditions Under Which FDA Can Disclose the Existence of a 510(k) Submission

Under 21 C.F.R. § 807.95(b), FDA cannot publicly disclose the existence of a 510(k) submission for a device that is not on the market and where the intent to market the device has not been disclosed if three requirements are met:

- the submitter must request in the submission that FDA hold as confidential commercial information the intent to market the device;
- FDA agrees that the intent to market the device is confidential commercial information; and
- the submitter must certify as to the confidentiality of the information and that neither he nor anyone else has disclosed the intent to market the device, that he will immediately notify FDA if he discloses his intent to anyone who is not an employee, paid consultant, or member of a hired advertising or law firm, and that he understands that the submission of false information to the government is illegal.

21 C.F.R. § 807.95(b). If the requirements of section 807.95(b) are met, FDA cannot disclose the existence of the 510(k) submission for 90 days after FDA receives a complete 510(k) submission. *See* 21 C.F.R. § 807.95(c)(1). If FDA requests additional information regarding the submission, the existence of the device will not be disclosed until 90 days after FDA receives the complete submission. Preamble to Establishment Registration and Pre-market Notification Procedures, Final Rule, 42 Fed. Reg. 42520, 42524 (Aug. 23, 1977) ("if the Commissioner requests additional information regarding the device under § 807.87(h), the existence of the device will not be disclosed until 90 days after the agency's receipt of a complete premarket notification submission.")

On November 26, 2008, GE Healthcare submitted a 510(k) requesting CDRH clearance of a new CT colonography screening indication for its CT Colonography II image analysis software visualization device, a computerized tomographic colonography device for virtual colonoscopies. In this 510(k) submission, GE Healthcare requested CDRH clearance to permit promotion of GE CT scanning devices for CT colonography screening. CDRH received the submission on December 1, 2008, and assigned it number [REDACTED]

When GE Healthcare submitted its 510(k), CT colonography screening was not being marketed. The use is still not on the market today. GE Healthcare did not disclose the existence of its 510(k) submission to any individuals who were not employees, paid consultants, or members of advertising or law firms hired under arrangements safeguarding confidentiality. GE Healthcare still has not revealed its submission for CT colonography screening. In its submission, GE Healthcare requested that CDRH hold as confidential commercial information its intent to market CT colonography screening and made all certifications required under section 807.95(b). CDRH did not object to GE Healthcare's request. Because GE Healthcare met all the requirements of section 807.95(b), CDRH was not permitted to reveal the existence of GE Healthcare's 510(k) submission for 90 days. GE Healthcare requested this confidentiality because it did not want its competitors to know that it was seeking this clearance, or create

April 16, 2010

Page 3

confusion in the marketplace as to the cleared indications for the currently marketed device. Those goals are now lost.

GE Healthcare has responded to numerous formal and informal requests for additional required information from CDRH since GE Healthcare submitted its 510(k) submission in November 2008. CDRH informed GE Healthcare in December 2009 that it will be issuing another request for additional information, which GE Healthcare is currently anticipating. In asking for additional information, FDA is effectively stating that GE Healthcare's premarket submission is not complete. According to section 807.95(c)(1), requests for additional information reset the 90 day period in which FDA is required to keep the existence of a 510(k) submission confidential because the period does not begin until FDA receives a *complete* premarket notification submission. CDRH is not permitted to reveal the existence of GE Healthcare's submission until the submission is complete, so in revealing the existence of GE Healthcare's submission while still asking for additional information, CDRH has breached the confidentiality requirements of 21 C.F.R. § 807.95.

## II. Conditions Under Which FDA Can Disclose the Contents of a 510(k) Submission

Data or information submitted with or incorporated by reference in a submission are not publicly disclosable until the intent to market the device is no longer confidential. 21 C.F.R. § 807.95(e); *see also* Preamble to Establishment Registration and Premarket Notification Procedures, Final Rule, 42 Fed. Reg. at 42525 ("Once FDA can disclose the fact that a premarket notification exists, the contents of the submission (other than information protected under § 807.95(e)) will be available for public disclosure."). FDA thus cannot disclose the contents of a 510(k) submission until it can disclose the fact that the submission exists. Certain information is exempt from disclosure even after the intent to market the device is revealed, such as confidential commercial information or safety and effectiveness data that have not already been disclosed to the public. *See id.*; Trade Secrets and Commercial or Financial Information Which Is Privileged and Confidential, 21 C.F.R. § 20.61(c) (2009). Once FDA makes a final classification decision, safety and effectiveness information in the submission are available to the public upon request, unless the device is a Class III device. *See* 21 C.F.R. § 807.95(e).

Because CDRH was not authorized to disclose the existence of GE Healthcare's 510(k) submission, it was not authorized to disclose the contents of GE Healthcare's submission either. CDRH has not yet made a final classification decision regarding CT colonography screening, and GE Healthcare still has not revealed its intent to market the use, so information in the submission is not available for public disclosure and should not have been released to the *New York Times*.

## III. Freedom of Information Act Procedures for FDA Disclosure of Information Relating to 510(k) Submissions

When FDA is authorized to disclose the existence and/or contents of a 510(k) submission to the general public, it may do so only in response to a specific written request for disclosure under the Freedom of Information Act ("FOIA"). *See* Policy on the Disclosure of Food and Drug Administration Records, 21 C.F.R. § 20.20(c) (2009); Establishment Registration and

WDC\_IMANAGE-1455066.1

Premarket Notification Procedures, Final Rule, 42 Fed. Reg. at 42524, 42525; FOOD AND DRUG ADMINISTRATION, FDA STAFF MANUAL GUIDES § 3297.1-7A (2007). We are unaware that any such request was received and processed with regard to GE Healthcare's 510(k).

FOIA requests for information in 510(k) submissions that meet the requirements of section 807.95(b) fall within a FOIA exemption for records containing trade secrets and confidential commercial information ("Exemption 4"). Confidential commercial information is any "valuable, non-public data or information relating to businesses, commerce, trade, employment, profits, or finances." FDA STAFF MANUAL GUIDES § 3297.1-7G(4). Records containing confidential commercial information are subject to predisclosure notification ("PDN") and must be withheld or redacted before release. See *id.* at § 3297.1-7G.

Under PDN procedures, FDA is supposed to make reasonable efforts to notify a submitter of a FOIA request for information in the submitter's 510(k) if the submitter has designated that the submission be protected as confidential commercial information, or if FDA has reason to believe that disclosure could reasonably be expected to cause substantial competitive harm to the submitter. See Exec. Order No. 12,600 § 8(d), 52 Fed. Reg. 23781 (June 25, 1987); 21 C.F.R. § 20.61(e)(1); Confidentiality of Information, Final Rule, 59 Fed. Reg. 64287, 64289, 64290 (Dec. 14, 1994); FDA STAFF MANUAL GUIDES § 3297.1-8L. FDA practice is to provide the submitter with a copy of the request and 510(k) submission prior to release so that the submitter can object to disclosure by redacting any trade secrets or confidential commercial information from the submission. See 21 C.F.R. § 20.61(e)(1); FDA STAFF MANUAL GUIDES § 3297.2-7B(6)(A). The submitter has five days to object to the requested disclosure. 21 C.F.R. § 20.61(e)(2). If FDA decides to disclose the information despite a submitter's objections, it must inform the submitter of why it did not sustain his objections. See 21 C.F.R. § 20.61(e)(3). No such efforts were made in this case, although it is our experience that FDA always follows these procedures.

There is no evidence that the *New York Times* made any FOIA requests for information relating to GE Healthcare's submission. Even if it had, it is unlikely that the information requested would have been furnished so quickly because FOIA requests generally take several months to years for FDA to process. See Eric P. Raciti and James D. Clements, *A Trap for the Wary: How Compliance with FDA Medical Device Regulations Can Jeopardize Patent Rights*, 46 IDEA 371, 379 (2006). Even if the *New York Times* had made a FOIA request, GE Healthcare should have been notified of the request and given a chance to object to the disclosure because the request involved confidential commercial information. However, at no time was GE Healthcare informed of the request or disclosure until it was contacted by *New York Times* reporter Gardiner Harris on March 25, 2010. By not waiting for a FOIA request before disclosing information in GE Healthcare's submission and not allowing GE Healthcare a chance to object even if the *New York Times* had made a FOIA request, CDRH acted in violation of both federal regulations and internal agency procedures when disclosing information in GE Healthcare's 510(k) submission.

#### IV. Conclusion

While FDA generally favors public disclosure of information, specific conditions constrain when FDA, and therefore, CDRH, can disclose information relating to 510(k)

April 16, 2010  
Page 5

submissions. FDA may only disclose the existence of a 510(k) submission for a device that is not on the market and where the intent to market the device is not public if the submitter has not designated the submission as confidential or made the proper certifications, or FDA disagrees with the designation. Otherwise, FDA must wait 90 days to disclose the existence of the 510(k). If FDA asks the submitter for additional required information, it cannot reveal the existence of the 510(k) even after 90 days have elapsed, because the confidential period does not start until FDA receives a complete submission. FDA cannot reveal the contents of a 510(k) until it can disclose the existence of the submission, such as when the intent to market is no longer confidential, or after FDA makes a final non-Class III classification decision. Even when the existence or contents of a submission are disclosable, FDA will not disclose information until it has received a specific written request and given a submitter notice of the request and a chance to object to the disclosure.

None of the conditions permitting FDA and CDRH to reveal the existence or contents of GE Healthcare's 510(k) submission were present when CDRH disclosed information to the *New York Times*. Even if they were, GE Healthcare was not given a chance to object to the release of confidential information in its submissions, in violation of federal regulations and internal agency procedure.

The confidentiality of 510(k) submissions is protected by federal regulations that resulted from extensive public discussion and comment. In creating these regulations, FDA's goal was to balance the need for the fullest possible government disclosure with the property rights of persons in confidential commercial information and the agency's need for frank internal policy deliberations. See 21 C.F.R. § 20.20(a). A breach in the confidentiality of 510(k) submissions upends the balance FDA has stricken between the need of companies to protect information that could cause competitive harm and the need of the public for government transparency. CDRH's release of internal documents such as emails and minutes of meetings also jeopardizes FDA's stated goal of protecting "the need for the agency to promote frank internal policy deliberations and to pursue its regulatory activities without disruption." 21 C.F.R. § 20.20(a). By disclosing information in GE Healthcare's submission in violation of these regulations, CDRH has disrupted this fine-tuned balance of interests and sacrificed pressing private and governmental needs in the name of unwarranted public disclosure.

Your prompt attention to this matter would be greatly appreciated. I will be contacting your office to schedule a meeting to discuss this matter.

Sincerely,



Edward M. Basile

cc: Dee Mellor, Chief Quality Officer, GE Healthcare  
Patricia Kaeding, Chief Regulatory Counsel, GE Healthcare

WDC\_JMANAGE-1455056 I



March 13, 2013

The Honorable Charles E. Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20515

Dear Senator Grassley:

Thank you for your letter of July 24, 2012, concerning the unauthorized disclosure of Food and Drug Administration (FDA) documents through a publicly accessible server operated by Quality Associates, Inc. (QAI). FDA and Department of Health and Human Services (Department) staff provided your staff, and staff of the House Committee on Oversight and Government Reform, a briefing on this matter on September 14, 2012. For purposes of this written response, Dr. Hamburg asked that I respond on her behalf because the business arrangement with QAI involved the Department of Health and Human Services (Department).

As we have previously advised, both the Department and FDA take seriously the unauthorized disclosure of sensitive personal information, confidential commercial information, and trade secrets entrusted to us. The Department is required to investigate security breaches in order to minimize the risk to the Department and individuals affected, and conducted such an inquiry in this case. The results of our internal review are included in the attached written responses to your specific questions. We apologize for the delay in providing you this follow-up written response, and appreciate your patience in this regard.

It is important to note that the FDA and the Department of Health and Human Services Program Support Center (PSC), which handled the Government Printing Office (GPO) contracting vehicle for the QAI task order, went to great lengths in attempting to protect the material in question from improper disclosure. At all times while the data was in the custody of the FDA and the PSC, it was securely maintained on an encrypted, 12-digit passcode-protected external hard drive. Data stored on the hard drive included, among other things, confidential commercial information, which the FDA is obligated to protect under federal law.

FDA requested the PSC's assistance in arranging for the conversion of the securely stored data to readable and printable format. FDA indicated to the PSC that the materials

The Honorable Charles E. Grassley  
Page Two

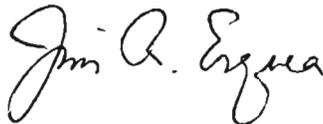
were highly sensitive and requested that the copying job be assigned a contractor that had prior experience with large copying jobs of sensitive and confidential documents. The PSC designated QAI under a Simplified Purchase Agreement (SPA), a streamlined printing procurement vehicle used by the GPO's customer agencies in the Executive Branch.

The PSC advised QAI that the documents were sensitive and that access to them should be limited. The PSC further requested that QAI delete all files on its computers after completing the job, and shred any printed documents in its possession. Regrettably, despite these instructions, QAI's unauthorized use of an unsecure website caused QAI to lose control of the confidential material. Although the PSC reviewed this matter with the GPO's Contracting Officer, unfortunately, the GPO's formal complaint process is limited to reports of poor printing quality, and is not designed to address security breaches.

Again, we share your concern about the data breach that occurred here. Any unauthorized use, disclosure, or loss of confidential information, such as the breach that occurred here, has the potential to undermine the public's trust and confidence in the Department's ability to properly protect such material, a matter we take quite seriously.

We would be happy to answer any further questions you may have.

Sincerely,



Jim R. Esquea  
Assistant Secretary for Legislation

Enclosure

RESPONSES TO SENATOR GRASSLEY'S QUESTIONS REGARDING  
QUALITY ASSOCIATES, INC. WORK ORDER 69308

- 1. Please provide and describe all communications to Quality Associates regarding the file converting contract, DHHS\FDA work order 69308.*

The first direct contact between personnel of the Food and Drug Administration (FDA or Agency) and Quality Associates, Inc. (QAI) regarding the work performed under this contract occurred on July 13, 2012, when FDA learned from a reporter that confidential Agency records appeared to have been released to the public.

In late April, 2012, individuals in FDA's Office of Information Management contacted the Program Support Center (PSC) of the Department of Health and Human Services (HHS), to request its assistance in arranging for certain FDA records to be organized and produced, in portable document format (PDFs), and printed. FDA personnel hand-delivered these records to the PSC on April 30, 2012, on an encrypted, 12-digit passcode-protected external hard drive. FDA requested that PSC utilize a contractor with proven experience handling sensitive information, and with whom PSC had a strong confidentiality agreement. The PSC later arranged for the data to be delivered to QAI via the same secure hard drive. For added security, FDA separately conveyed the 12-digit passcode to the PSC by telephone.

The PSC initially engaged a different firm, Ideal Scanners and Systems Inc. (Ideal), to organize and produce material from files stored on the FDA's encrypted hard drive in PDFs. On May 1, 2012, Ideal personnel picked up the hard drive and took it to Ideal's facilities. However, after Ideal obtained the 12-digit passcode from the PSC, Ideal determined that it lacked the technical capability to convert all of the hard drive data to PDFs. The next day, Ideal contacted the PSC Printing Specialist, who was on-site at QAI at the time for unrelated reasons. After the Printing Specialist and QAI conferred by phone with Ideal, QAI indicated that it could meet the technical and expedited time requirements for the job.

The FDA had requested that the job be completed within 72 hours, by Friday, May 4, 2012. The Printing Specialist verbally informed QAI that this was a "sensitive job" involving litigation and was to be treated as such, including by ensuring the files were handled by as few staff as possible and removed from computers when the job had been completed. QAI sent a courier specifically cleared to handle sensitive data to pick up the hard drive from Ideal. Moreover, Ideal gave QAI the passcode verbally.

The PSC did not authorize QAI to load the files on a publicly accessible file transfer protocol (FTP) site. Although QAI shared with the PSC a link to its FTP site with the first set of PDFs it generated, FTP sites may be shielded from public view through at least two techniques: (1) password protection and (2) "locking down." Thus, QAI's reference to its use of an FTP site failed to alert the PSC that documents would be publicly available. Indeed, neither the PSC nor FDA were aware that the material was available on a publicly accessible network until a reporter for the New York Times informed the FDA of this fact on July 13, 2012.

QAI completed the job on May 9, 2012. The PSC documented the work done by QAI, which included organizing, bates-stamping, and converting data to PDFs, as part of Work Order 69308 on May 23, 2012.

Unfortunately, the GPO's required Work Order forms do not reflect the variety of confidential material frequently handled by Executive Branch agencies, including material as to which Congress has imposed specific statutory protections. The forms provide only three document category options: a) Classified; b) SBU (sensitive but unclassified); and c) PII (personally identifiable information). Other options for identifying protected information, such as confidential commercial information, are not available on GPO's Work Order form.

Although the FDA hard drive in fact contained PII (one of the designated options on the form), the Work Order that the PSC later submitted to document the job order inadvertently indicated that the material did not contain PII. Notably, however, this erroneous documentation occurred after QAI had completed its work, and, therefore, could not have contributed to QAI's unauthorized disclosure of FDA's sensitive and confidential data.

- 2. Prior to May 23, 2012, did FDA represent to Quality Associates that the files submitted for conversion contained no information that was classified, SBU, or PII? Please describe all communications with Quality Associates regarding the nature of the documents to be converted and provide all records relating to those communications.*

As noted above, FDA had no direct contact with QAI prior to the completion of QAI's work in this matter. The PSC verbally informed QAI on May 2, 2012, the same day work on the job commenced, that this was a "sensitive job" involving litigation and was to be treated as such, including by ensuring the files were handled by as few staff as possible and removed from computers when the job had been completed. The fact the data was delivered on an encrypted, 12-digit passcode-protected external hard drive reinforced the extra security precautions that the PSC expected QAI to take. The PSC's Printing Specialist also asked QAI to shred any documents they had in their possession derived from the work.

- 3. Why was Quality Associates allowed to begin work without an authorizing work order? Was the work completed on a rush basis, and if so why?*

The PSC and the vendor were attempting to accommodate the FDA's request for expedited delivery; i.e., to have the job completed and delivered to FDA within 72 hours.

- 4. Please explain the timeline as to when Quality Associates actually performed services for the federal government. More specifically, please clarify how Quality Associates claims that the files were uploaded on May 3, archived on May 9, the order was placed on May 21, and the work order was approved May 23.*

QAI received the job from PSC on May 2, 2012, and completed it on May 9, 2012. The final print order was generated afterward. While the initial request was for approximately 10,000 files of various sizes in approximately 1,000 folders on a hard drive to be converted to PDFs for purposes of printing, the number of PDF pages requested to be converted, and the formatting of the job, changed several times during the process, thereby delaying delivery on the initially requested date of May 4, 2012.

5. *Who was responsible for initiating the work order eventually received by Quality Associates? Please provide the originating document(s).*

The Printing Specialist for the PSC was responsible for initiating the print order. The originating document is Work Order 69308 (attached to your letter).

6. *Were there any additional employees, either within FDA, the Government Printing Office (GPO), or any other federal agency responsible for passing along the details of the Quality Associates work order? Please provide the information about the documents related to all of the steps required from the originating document until the purchase agreement is considered complete.*
  - a. No additional employees within FDA, or any other executive branch agency, or GPO, were responsible for passing along details of the QAI work order.
  - b. A completed HHS-26 Form is the originating document for a print order. If an HHS-26 is not accessible, a customer may email its job requirements and method of payment to initiate work on the part of the Program Support Center. On May 2, 2012, the Program Support Center received the final set of requirements from FDA, including the funding information.
  - c. We note that the work order and invoices were included with your letter. Attached hereto are the terms and conditions and instructions for completing the 4044.
7. *Who was responsible for preparing the "Simplified Purchase Agreement Work Order Form 4044" for Quality Associates' DHHS\FDA work order no. 69308? Where did that person obtain the information contained within the document?*
  - a. For Work Order 69308, the PSC Printing Specialist was responsible for filling out the Simplified Purchase Agreement Work Order Form 4044.
  - b. FDA provided information to PSC regarding the nature of the documents. Although this information was not fully reflected on the completed form, the form was not prepared until after the work was done. Nonetheless, PSC did convey the sensitive nature of the information to QAI orally, before it undertook the work.
8. *Does the FDA still maintain that the documents provided to Quality Associates contain no information that is classified, SBU, or defined as PII under the Privacy Act?*

The FDA and HHS have never maintained that the hard drive contained no personally identifiable information. The absence of such a notation on the later-completed work order was the result of a clerical error at the PSC.

9. *What litigation was this document conversion being prepared for? Were the documents being prepared for production or merely for review in order to determine what would and would not be produced?*

At the time QAI was engaged to convert the FDA data into a readily printable form, concerns related to the computer monitoring of certain current and former FDA personnel were already the subject of Congressional and Office of the Special Counsel (OSC) investigations, as well as litigation. The printing was principally intended to enable review of these records to facilitate understanding facts thought to be potentially relevant to these matters, and not for production in response to a specific request.

10. *Quality Associates asserts that the original files were initially supplied on physical media to another contractor. What is the name of the other contractor?*

The original contractor requested to perform this work was Ideal Scanners and Systems Inc. Ideal was unable to perform the work.

11. *How many files were contained on the physical media?*

The PSC did not open the files on the media provided; however it is estimated to be ~ 10,000 files per emailed requirements.

12. *What was the total number of pages provided from Quality Associates to FDA following the conversion?*

The total number of pages provided from QAI following the conversion to PDF was 83,187. Three copies were printed and delivered to FDA.



July 17, 2012

United States Senate  
Committee on the Judiciary  
Attn: Senator Grassley  
Washington, DC 20510-6275

RE: Letter received on July 16<sup>th</sup> (attached)

Quality Associates, Inc. is extremely concerned by your letter and would like to address your questions. We have also contacted your staff in the interest of providing information and clearing any misunderstandings that we have done anything other than follow our Clients directions.

Please see the following answers to your questions:

1) With how many government agencies does Quality Associates have contracts?  
Please provide the total dollar amount for each agency.

Response – QAI has hundreds of government Clients and the dollar values for each range from hundreds of dollars (for product purchases) to millions of dollars for multi-year support contracts.

2) Which of these other agencies' internal information, if any, was accessible through the Internet prior to Friday afternoon?

Response – The FTP site is used to make available conversion tools (script files, custom coding, etc.) and DLL files for our engineers to download and implement at client sites. Occasionally, we have Clients that request files and, with their approval, we use the FTP site for the transfer.

3) Why were these internal documents publicly available and searchable on search engines, such as Google?

Response – The files were put on our FTP site at the direction of our Client. During the time that they were there the files were “crawled” by the Google engines.

4) What services, specifically, do you provide for each of these agencies?

Response – Quality Associates Inc. (QAI), a Maryland based Small Business, was established in 1986 as a Quality Assurance (QA) Good Laboratory Practice (GLP) consulting company to



QUALITY  
ASSOCIATES  
INCORPORATED

provide services to the pharmaceutical, pesticide, and other appropriate chemical and biotech industries. In the late 1990's, QAI started to focus more on the Federal marketplace, primarily with the regulatory/research agency's who required day-to-day business solutions for turning paper-based information into usable electronic data. In recent years, QAI has expanded its client relationships to include educational, healthcare and banking customers and is now providing full document/content management solutions based on the Microsoft SharePoint ECM platform.

5) Has Quality Associates ever discovered a similar leak as the one identified in The New York Times article? If yes, please provide a detailed explanation of each instance.

Response - Never.

6) How long were the FDA documents publicly available on Quality Associates Internet site?

Response - The files were first uploaded to the site, at the direction of our Client, late in the evening on May 3<sup>rd</sup>. There were several iterations of file revision and reloading to help our Client with their printing of the files. The last day that we worked with our Client and these files was on May 9<sup>th</sup>. Our records show that the files were archived on May 9<sup>th</sup>.

7) What steps have you taken to ensure that such internal information is not inappropriately available online in the future?

Response - We have removed the FTP site and will handle all future receipt and delivery of Client information, regardless of Client direction, via physical pick-up/delivery and/or secure/encrypted transfer.

Sincerely,

Paul Swidersky  
President, CEO

**Simplified Purchase Agreement  
Work Order Form 4044**

You are hereby authorized to manufacture and ship the following described product in accordance with the purchase order and

QUOTES DUE BY

DEPARTMENT DHHS/FDA	REQ. NO. 2-06004-	JACKET NO. 372-628	BPA NO. 960	WORK ORDER NO. 69308
CLASSIFICATION Classified <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No SBU <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No PII <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	PUBLICATION TITLE LITIGATION FILE ORGINAZATION		DATE PREPARED 05/23/2012	OBJECT CLASS
CONTRACTOR Quality Associates Inc	PURCHASE ORDER NO. 96645	STATE CODE 190	CONTRACTOR'S CODE 72508	SHIP/DELIVERY DATE 5/25/2012

NOT FOR CONTRACTOR	BILLING ADDRESS CODE (BAC) 4164-01	AGENCY LOCATION CODE (ALC) 75060099	APPROPRIATION CHARGEABLE/OBLIGATION NO. 69999WC
	Pay by <input type="checkbox"/> Purchase Card <input type="checkbox"/> Purchase Card	PURCHASE CARD NO. (Info to Appear on GPO Copy Only)	EXP. DATE
	PHONE NO. OF CARDHOLDER	EMAIL OF PURCHASE CARDHOLDER	TREASURY ACCOUNT SYMBOL (TAS)
	LINE OF ACCOUNTING REFERENCE NUMBER (Info Will Appear on IPAC as Entered) 2000061		

SPECIFICATIONS	PROOFS <input type="checkbox"/> Contact <input type="checkbox"/> Inkjet <input type="checkbox"/> High Resolution <input type="checkbox"/> Prior to Production Samples <input type="checkbox"/> Electronic Soft Proof	DAYS DEPT. WILL HOLD PROOFS	QUALITY LEVEL	QUANTITY 0
	FURNISHED ELECTRONIC MEDIA <input type="checkbox"/> Files to be sent via FTP or Email <input type="checkbox"/> CD/DVD	OTHER GOVT. FURNISHED MATERIALS	PRESS SHEET INSPECTION <input type="checkbox"/> No. of Hours Notice	TRIM SIZE
	COVER PAPER	COLOR OF COVER INKS	COVER COATING TYPE	PAPER COVERS (Self) (Separate)
	TEXT PAPER	COLOR OF TEXT INK	TEXT COATING TYPE	NUMBER OF TEXT PAGES 0
	STITCH <input type="checkbox"/> U/LC <input type="checkbox"/> SIDE <input type="checkbox"/> SADDLE	BINDING <input type="checkbox"/> COMB <input type="checkbox"/> COIL <input type="checkbox"/> PERFECT BOUND <input type="checkbox"/> SEW <input type="checkbox"/> TAPE	INDICATE WHICH COVERS PRINT 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/>	

ADDITIONAL INFORMATION	Description	<input type="checkbox"/> Supplemental information Attached
	Organize and brine number 68,000 files. Create pdf's and email to address supplied. Please send email to [redacted] when job is delivered.	
	GFM, Negs, Samples to JAMES HELTON, 6600 Fishers Lane, Parkawn Bldg. Room [redacted], Rockville, MD 20857. [redacted] **Delivery hours for the Parkawn Building are 8:30 am to 12:30 pm - 1:00 pm to 4:00 pm. Deliveries must be made at loading dock.**	
	All invoices are to be sent to: U.S. Government Printing Office, Office of the Comptroller, STOP FMC5, Washington, DC 20401 or faxed to 202-[redacted] include program and work no. on labels to insure proper payment.	

DELIVERY	DELIVER PRODUCT TO:	RETURN FURNISHED MATERIAL TO:
	<input type="checkbox"/> Distribution List Attached	Digital Deliverables Requested - Format: <input type="checkbox"/> Native <input type="checkbox"/> PDF

SUPT. DOCS. NOTIFIED <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	SUPT. DOCS. QUANTITY ORDERED	SUPT. DOCS. DELIVERY ADDRESS
CONTRACTOR TOTAL QUOTE \$4,000.00	SUPT. DOCS. COST	ADDITIONAL RATE

FOR ADDITIONAL INFORMATION CONTACT:	EMAIL	PHONE NO.	FAX NO.
-------------------------------------	-------	-----------	---------

AUTHORIZING SIGNATURE (must be on file with GPO)	DATE SENT TO CONTRACTOR 5/23/2012
ORDER RECEIVED BY: (Agency Representative)	DATE ORDER RECEIVED 5/23/2012

CONTRACTOR INVOICE	All contractor invoices are to be FAXED to GPO at 202-[redacted]. For instructions on how to prepare your bill and get paid go to <a href="http://www.gpo.gov/vendors/payment.htm">www.gpo.gov/vendors/payment.htm</a>
	I certify that the materials/services ordered have been delivered on the date indicated above and that payment or credit has not been received. The penalty for making false statements to the Government is prescribed in 18 USC 1001.
CONTRACTOR SIGNATURE	DATE

THIS FORM MUST BE FURNISHED TO GPO UPON SUBMISSION TO CONTRACTOR

APRIL 2010

Work Description, May 2012



Quality Associates, Inc.

8161 Maple Lawn Blvd, [REDACTED]

Maple Lawn, MD 20759

Fax: [REDACTED]

Tel: [REDACTED]

Provided To:

[REDACTED]  
Printing Specialist, Pub Mgmt Branch  
Div of Support Services  
Program Support Center  
5600 Fishers Lane, Room [REDACTED]  
Rockville, MD 20857

Date: 5/21/2012

PSC Contact:

Project: Conversion Services

Agency: PSC - Div of Support Services

PSC Contact Phone: 301-[REDACTED]

Email:

Prepared By

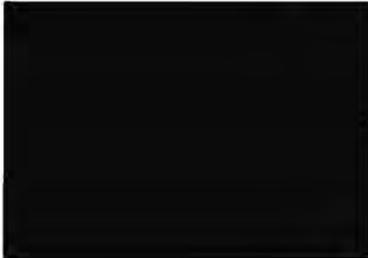
Name:

Phone:

1	Analyze data from client supplied hard drive. Convert files from various formats to pdf for printing	1	\$4,000.00	\$4,000.00
			<b>SUBTOTAL</b>	<b>\$ 4,000.00</b>

**Total Order** \$ **4,000.00**

Notes:



5/23/2012  
Date

- Payment terms are net 30 days.

Laptop Name - DRL0098686

Spector Client: installed and active since 4/22/10

SUBJECT: Robert C. Smith (RCS)  
Medical Officer  
WO66 RM0319G HFZ-470  
CDRH - ODE/DRARD

Search Terms:

Colonography - SUBJECT feels the FDA is not handling this issue well.

Allegations:

Sending proprietary documents and information out of the FDA. Some documents are may have the letter "K" followed by a string of six (6) numbers. Check to see if SUBJECT is sending these outside the FDA. Probably using Gmail to send out.

SUBJECT sent proprietary documents to press, possibly NY Times (Gartner Harris - sp?) - (Gardiner Harris - Corrected) for article alledging the FDA was mis-handling the Colonography topic.

His superiors believe HE is "ghost writing" his subordinates FDA reports. Check all possible avenues for possible occurances.

SUBJECT'S subordinates or co-horts:

[REDACTED]	DRL0091494
Paul T. Hardy	DRL0102315
[REDACTED]	DRL0101046 DRL5125449
Cindy Demian	DRL0101600
Nancy Wersto	DRL5114924
Lakshmi Vishnuvajjala	DRL5125617 DRL0096322

Check all for possible POP3 or enternal, non-FDA email conversations, either via Websense, Encase, Mandiant, or Spector.

## Actors List:

### Primary Actors

1. Robert C. Smith – Medical Officer, CDRH, ODE/DRARD  
WO66, [REDACTED], 10903 New Hampshire Ave, Silver Spring, MD
2. Paul T Hardy (also referred to as “PJ”) – Regulatory Review Officer, CDRH,  
OIVD  
WO66, [REDACTED] 10903 New Hampshire Ave, Silver Spring, MD
3. Julian J. Nicholas – Former CDRH Physician

Summary – The above listed actors appear to be the point men. All communications amongst all the actors filter through one or all of these three primary actors. These actors appear to perform the majority of any review, editing, compilation, production or distribution of verbiage, documentation and information. Actors 1 and 3 appear to have the greatest involvement with media outlets and external organizations.

### Secondary Actors

4. Ewa M. Czarska ~ Biologist, CDRH, ODE/DRARD  
WO66, [REDACTED] – 470, 10903 New Hampshire Ave, Silver Spring, MD
5. [REDACTED] – Visiting Scientist, CDRH, OSEL/DIAM  
WO62, [REDACTED], 10903 New Hampshire Ave, Silver Spring, MD
6. [REDACTED] – Biomedical Engineer, CDRH, ODE/POS/IDE  
WO66, [REDACTED], 10903 New Hampshire Ave, Silver Spring, MD
7. Nancy Wersto – Biologist, CDRH, ODE/DRARD  
WO66, [REDACTED], 10903 New Hampshire Ave, Silver Spring, MD
8. Lakshmi Vishnuvajjala – SUPV. Mathematical Statistician, CDRH,  
OSB/DBS/DDB  
WO66, [REDACTED] – 550, 10903 New Hampshire Ave, Silver Spring, MD
9. [REDACTED] – Physicist, CDRH, ODE/DRARD  
WO66, [REDACTED] – 470, 10903 New Hampshire Ave, Silver Spring, MD

Summary – The secondary actors listed above are in constant communication amongst themselves and the primary actors via FDA email, Yahoo Mail and Gmail. Communications involve review, editing, compilation, production or distribution of verbiage, documentation and information pertaining to medical reviews, current investigations, claims against HHS/FDA, release of information to the press and external organizations.

### Ancillary Actors

10. Ned Feder – Staff Scientist / Writer – POGO (Project On Government Oversight)

1100 G Street, NW, Suite [REDACTED], Washington, D.C

11. [REDACTED] – Associate of Ned Feder  
Nuclear Engineering, Texas A&M University
12. Jack Mitchell - United States Senate, Special Committee on Aging  
G31 Dirksen or 628 Hart Senate Office Buildings, Washington, D.C.
13. Joan Kleinman – District Director, Congressman Chris Van Hollen (D-Md)  
Office of Representative, 51 Monroe Street #507, Rockville, Md.
14. Congressman Chris Van Hollen (D-Md)  
House of Representatives  
1707 Longworth H.O.B., Washington, D.C.  
District Office - 51 Monroe Street #507, Rockville, Md.

Summary – The ancillary actors above are actively participating with primary and secondary actors with regard to complaints and claims filed against HHS/FDA referencing FDA review / approval process, discrimination and hostility within the workplace. The above actors (with the exception of Congressman Chris Van Hollen and [REDACTED] directly) have received a substantial number of documents primarily from Actors 1 and 3. There has also been numerous communications with many of the secondary actors either directly or through the primary actors. References to one or more of the above ancillary actors providing a conduit to release information to the press has been identified.

#### Media Outlet Actors

15. Gardiner Harris – Reporter, New York Times
16. Matthew Perrone – Reporter, Associated Press
17. Alyah Khan – Reporter, Inside Washington Publishers news organization
18. Joe Bergantino – Reporter, RCN Cable Washington based Direct Cable provider
19. Rochelle ( last name unknown) – Associate of Joe Bergantino
20. Lainey Moseley – Journalist, Unknown Philadelphia news organization - looking for a “Bigger Story” on CT scans, patient safety and FDA recommendations
21. Joe (last name unknown) – Documentaries, Frontline PBS (Public Broadcasting Service)

Summary – The media outlet actors listed above have actively and recently communicated primarily with Actor 1. Actor 1 has been in constant contact with Actors 15, 16, 17, & 18 via email, phone communications and/or in-person meetings regarding “issues with in the FDA”. Actor 20 was referred to Actor 1 by Actor 3. Actor 21 has been referenced to Actor 1 by Actor 2.



FILE COPY

Food and Drug Administration  
Office of Internal Affairs (HFH-560)  
One Church Street, [REDACTED]  
Rockville, MD 20850

May 14, 2010

Scott A. Vantrease  
U.S. Department of Health and Human Services  
Office of Inspector General  
Office of Investigations  
Special Investigations Unit  
330 Independence Avenue, S.W.  
Washington, DC 20201

RE: GE Healthcare Complaint

Dear ASAIC Vantrease:

On April 23, the Office of Internal Affairs was given a copy of a complaint from King and Spalding, a law firm representing GE Healthcare. This complaint alleges disclosure of confidential information by unknown individuals at the FDA's Center for Devices and Radiological Health (CDRH).

As these allegations are very serious and to avoid any appearance of impropriety, I respectfully request that HHS/OIG/SIU investigate GE Healthcare's allegations. Because the OIG is entirely independent of the programs and officials being investigated, any potential allegations of conflict of interest by any party, or members of congress would be eliminated. Please contact me at (240) [REDACTED] if you wish to discuss this matter.

Sincerely,

A handwritten signature in cursive script, reading "Mark S. McCormack".

Mark S. McCormack  
Special Agent in Charge

Enclosure

Cc:  
Case File  
Chron



*Case Initiation and Fact Sheet*

Case Number: 2010-OIA-970-073 Case Title: GE Healthcare  
Case Type: Unauthorized Disclosure of Information Case Assignment:

**COMPLAINT:**

Date Received: 4/23/10 Person Receiving Allegation: SAIC McCormack  
Complaint-received by: Telephone: Letter: Other: X (email)

Name of Complainant: King and Spaulding, LLP  
Address: 1700 Pennsylvania Ave. NW, WDC 20006  
Telephone Number: [REDACTED]

Allegation and/or Issues: GE Healthcare alleges unauthorized disclosure of information by unknown FDA/CDRH employees. This allegation is being referred to HHS/OIG/SIU to remove any potential allegations of impartiality.

**SUBJECT(S):**

Grade:  
Title:  
Component:  
Region:  
Address:  
Telephone Number:

**Other Agency Involvement:**

OIG Notification: Telephone: Memorandum:  Fax:  
Date Notified: 5/17/10  
Person Notified: Scott Ventrease

**COMMENTS:**

SAIC Signature *Mark L. McCormack* Date: 5/14/2010



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General  
Office of Investigations  
Special Investigations Branch  
Washington, DC 20024

JUL 26 2012

Mr. Mark McCormack,  
Special Agent in Charge  
U.S. Department of Health and Human Services  
Food and Drug Administration  
Office of Criminal Investigations  
Office of Internal Affairs  
1 Church Street, [REDACTED]  
Rockville, MD 20850

RE: Case Name: Unauthorized Disclosure of Information  
OI File #: H-10-0-0141-3

Dear SAC McCormack:

I am writing to clarify our May 18, 2010, letter to you regarding your referral (OIA File #: 2010-OIA-970-073). First, the Office of Inspector General (OIG) does not determine the legality of disclosures of confidential government-held information. Instead, an OIG conducts investigations and refers matters to the Department of Justice when the OIG determines there are "reasonable grounds to believe" there has been a violation of Federal criminal law. (IG Act, § 4(d)). Our 2010 letter should not be read to reflect a determination by OIG about the reach of Federal criminal law. Again, that determination rests with the Department of Justice and the courts. OIG's May 2010 decision to take no further action on your referral was based on our assessment of the evidence available at that time under the standard set forth in the IG Act.

If you have any questions, or need any additional information regarding this matter, please feel free to contact me at [REDACTED]

Sincerely,

  
Elton Malone  
Special Agent in Charge  
Special Investigations Branch

Enclosure



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General  
Office of Investigations  
Special Investigations Branch  
Washington, D.C. 20201

MAY 18 2010

Mr. Mark McCormack,  
Special Agent in Charge  
U.S. Department of Health and Human Services  
Food and Drug Administration  
Office of Criminal Investigations  
Office of Internal Affairs  
1 Church Street, [REDACTED]  
Rockville, MD 20850

RE: Case Name: Unauthorized Disclosure of Information  
OI File #: H100001413

SAC McCormack:

The U.S. Department of Health and Human Services (HHS), Office of Inspector General (OIG), Office of Investigations (OI), Special Investigations Branch (SIB), is in receipt of your referral (OIA File #: 2010-OIA-970-073). At this time, based on the information provided, OIG/OI/SIB will be taking no action. The referral lacks any evidence of criminal conduct on the part of any HHS employee. Additionally, 5 U.S.C. § 1213, identifies that disclosures, such as the ones alleged, when they relate to matters of public safety may be made to the media and Congress as long as the material released is not specifically prohibited by law and protected by Executive Order or National Security Classification.

The OIG is appreciative of your support in its overall mission. Thank you for contacting the OIG on this matter. Should you have any questions, or need any additional information, please feel free to contact me at [REDACTED]

Respectfully,

Scott A. Vantrease  
Assistant Special Agent in Charge  
Special Investigations Branch

McKee, Ruth E

From: Marty, Kenneth L (OIG/OI) [REDACTED]  
Sent: Friday, June 10, 2011 1:37 PM  
To: McKee, Ruth E  
Subject: Complaint RE: Hardy et.al.  
Attachments: H100024830016a2449 20101115 Closing Memo to CDRH.pdf; H100024830015a2449 20101105 Declination Letter from DOJ PIN.pdf

Ruth,

The referral you made to our office in March of this year regarding the .wav files was subsumed into case H100002483 since it pertained to the same category of conduct.

Attached are previous documents our office transmitted to your office regarding that case. As in that instance, we are deferring to FDA for any appropriate administrative action.

If you need a more official letter from us, please let me know.

Sincerely,

*Kenneth Marty, Inspector  
Special Investigations Branch  
Office of Inspector General, Office of Investigations  
U.S. Department of Health & Human Services  
330 Independence Ave., S.W. [REDACTED]  
Cohen Bldg.,  
Washington, D.C. 20201*

*This E-mail may contain sensitive law enforcement and/or privileged information. If you are not the intended recipient (or have received this E-mail in error) please notify the sender immediately and destroy this E-mail. Any unauthorized copying, disclosure or distribution of the material in this E-mail is strictly forbidden.*

**From:** Mehring, David S (OIG/OI)  
**Sent:** Friday, June 10, 2011 10:27 AM  
**To:** Marty, Kenneth L (OIG/OI)  
**Subject:** Complaint from Ruth McKee

Ken,

Here's the additional complaint sent to us by Ruth McKee after we closed our investigation (H10002483), and my email response. I've also included DOJ/PIN's declination letter, and our case closing memo to CDRH.

Let me know if I can provide any further info, or assist with the response to CDRH.

Dave

David Mehring, Special Agent  
U.S. Department of Health and Human Services  
Office of Inspector General  
Special Investigations Branch  
Washington, DC  
[REDACTED]



FEB 23 2011

Daniel R. Levinson, Inspector General  
U.S. Department of Health and Human Services  
Office of Inspector General  
Washington, DC 20201

Re: Potential Unlawful Wiretapping By FDA Employee

Dear Mr. Levinson:

We have obtained evidence that at least two FDA employees appear to have engaged in widespread recording of telephone calls and meetings regarding FDA business without the consent of all other parties. We are concerned that these actions violated state and/or federal criminal laws. I have enclosed with this letter a draft summary of some of the recordings we have obtained, and I am sending all the recordings to you via your secure IT portal. Please review this information to determine whether the Office of Inspector General (OIG) will open an investigation.

In the course of network monitoring, we discovered 96 .wav files containing recordings of conversations the employees had with other FDA employees and with representatives of companies with matters pending before FDA. These .wav files were located on a thumb drive connected to an FDA computer in "unallocated space" indicating they had been "deleted" but not yet overwritten. The recordings themselves suggest that they were made by two different employees, and the recordings also suggest that many of the participants were not aware that they were being recorded. The subject matters of these recorded calls and meetings include the review of pending medical device submissions, FDA personnel matters, and efforts of the employees to use the press and Congress to force the removal of specified FDA managers. These recordings include non-public information, some of which appear to constitute confidential commercial information. For instance, Files 16 and 17 are recordings of conversations with a manufacturer regarding a device submission. Although the files we have obtained do not specify the dates or times of the calls themselves, we expect, based on the context and subject matter of the recordings, that the calls generally took place between 2008 and 2010.

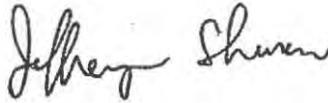
The employees seem to have been in several different physical locations, all of which were likely in the State of Maryland, when they made the recordings. In particular, the recordings suggest that they were variously recording the calls and meetings from their FDA offices (in White Oak, Maryland or Rockville, Maryland), and from coffee shops near the FDA offices.

There is no FDA policy or practice that supports the unauthorized taping of phone calls or meetings by employees, or the use of FDA equipment or resources for such purposes.<sup>1</sup> Moreover, the creation and storage of these recordings might run afoul of the requirements relating to the secure storage and destruction of sensitive information and prohibitions against the concealment of such information for personal use; these requirements are contained in the Department of Health and Human Services Rules of Behavior For Use of Technology Resources and Information, which all employees must read and sign.

More significantly, these nonconsensual recordings potentially violate state or federal criminal wiretapping laws. For example, Maryland law prohibits the interception of oral or electronic communications unless "*all of the parties* to the communication have given prior consent to the interception...."<sup>2</sup> Violations are felonies subject to imprisonment and fines.<sup>3</sup> Federal law appears to require the consent of only one party to the interception of a phone call,<sup>4</sup> but the unauthorized taping of calls by federal employees involving confidential information may constitute prohibited conduct.

If you have any questions, or if you need any additional information, please let me know.

Sincerely,



Jeffrey Shuren, M.D., J.D.  
Director  
Center for Devices and  
Radiological Health

Enclosure

---

<sup>1</sup> FDA regulations generally allow the recording of public administrative proceedings, with advance notification to the agency. See 21 C.F.R. § 10.204. None of the calls at issue here appear to constitute public administrative proceedings.

<sup>2</sup> Md. COURTS & JUDICIAL PROCEEDINGS Code Ann. § 10-402(c)(3) (emphasis added). Other exceptions apply, which do not appear to be relevant here.

<sup>3</sup> *Id.* § 10-402(b).

<sup>4</sup> See 18 U.S.C. § 2511.



Office of the Chief Counsel  
Food and Drug Administration  
10903 New Hampshire Avenue  
Silver Spring, MD 20993-0002

TO: Walter Harris, Chief Operating Officer  
Eric Perakslis, Chief Information Officer

FROM: Elizabeth H. Dickinson, Chief Counsel *E.H.D.*

RE: Requirments for Deploying Spector Software

DATE: August 1, 2012

**Effective immediately -**

Per the direction of Commissioner Margaret A. Hamburg, the FDA Office of Information Management will not deploy the Spector 360 software without written approval by the Chief Counsel or her delegee. The Chief Information Officer is to immediately instruct his staff accordingly.

Questions on this policy are to be directed to Elizabeth Dickinson, Chief Counsel.

cc: Margaret A. Hamburg, Commissioner of Food and Drugs  
Lisa Barclay, Chief of Staff  
John M. Taylor, III, Counselor to the Commissioner  
Mark Raza, Acting Deputy Chief Counsel



DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration  
Silver Spring, MD 20993

FROM: Margaret A. Hamburg, Commissioner

TO: Walter Harris, Chief Operating Officer  
Eric Perakslis, Chief Information Officer  
Elizabeth H. Dickinson, Chief Counsel

RE: Monitoring of FDA Personnel Work Computers

DATE: September 24, 2012

The Food and Drug Administration has recently undertaken a review of the standards and procedures for monitoring the use of government-owned computers issued to FDA personnel. After careful consideration, I am issuing additional guidance to ensure that such activity continues to be conducted in an appropriate manner.<sup>1</sup> Accordingly, I am directing the FDA Chief Information Officer (CIO) to put into place promptly procedures that will strengthen FDA's ability to effectively document, analyze, and authorize requests for employee computer monitoring.<sup>2</sup>

Pursuant to this memorandum, which is effective immediately, I am directing that the CIO and Chief Counsel<sup>3</sup> promptly develop a written procedure that includes the following elements:

**Express Written Authorization of Monitoring:** The CIO may not initiate monitoring of FDA employees' computers without advance written authorization by one of the following: The Commissioner, a Deputy Commissioner, or the Chief Operating Officer (COO). This authority may not be redelegated. Requests for monitoring must be approved by the Chief Counsel in writing prior to implementation, as described below.

<sup>1</sup> As an initial interim step, by Memorandum dated August 1, 2012, I directed that the FDA Office of Information Management will not deploy new uses of the Spector 360 software without written approval by the Chief Counsel or her delegee.

There are currently a number of inquiries into monitoring practices that will inform FDA's policies and practices and that may result in additional changes to FDA procedures in the longer term, including a Department-wide review requested by the Office of Management and Budget and two reviews by the HHS Inspector General requested by the Secretary. I will update FDA's policies as needed once those reviews are completed.

<sup>2</sup> This memorandum addresses the use of monitoring software directed at individual FDA computers issued to specific employees which operates by making a continuous record of activity on such computers; it is not intended to address standard information technology (IT) security controls employed throughout the FDA IT system to implement Federal Information Security Management Act of 2002. Other FDA information technology practices may raise legal and policy concerns similar to those identified in this memorandum. The CIO and Chief Counsel should develop procedures as necessary to address these as well.

<sup>3</sup> FDA's Office of the Chief Counsel is part of HHS' Office of General Counsel (OGC); I expect that in advising FDA, OCC will consult and work closely with other OGC experts and management.

**Basis for Monitoring:** Computer monitoring may be authorized only for the following reasons: (1) at the request of an outside law enforcement or national security authority (e.g., FBI, DHS) or the HHS Inspector General; (2) based on reasonable grounds to believe that the individual to be monitored may be responsible for an unauthorized disclosure of legally protected information, such as confidential commercial or trade secret information; or (3) based on reasonable grounds to believe that the individual to be monitored has violated HHS or FDA personnel or administrative policy or HHS or FDA policy on the use of government information technology equipment and systems.

**Documentation:** The written authorization for monitoring of FDA employee computers must describe the reason for the monitoring. If the monitoring is initiated at the request of an outside law enforcement or national security authority or by the HHS Inspector General, the authorization must state that the request was approved by the Director of FDA's Office of Criminal Investigation or by the HHS Inspector General, as appropriate.<sup>4</sup>

For monitoring that is initiated for reasons other than at the request of an outside law enforcement or national security authority or the HHS Inspector General, the party requesting the monitoring must document in writing the factual basis justifying the monitoring. The Chief Counsel shall document in writing the legal basis for any such monitoring.

**Limiting the Time, Breadth, and Invasiveness of Monitoring:** The written authorization for monitoring should reflect that the CIO has identified a method of computer monitoring that is as narrow, time-limited, and non-invasive as is appropriate to accomplish the stated information-gathering objective. The CIO also shall consider and advise on whether there are alternative steps the agency could take to address the concern.

When monitoring is initiated at the request of an outside law enforcement or national security authority or the HHS Inspector General, the CIO should, to the extent possible under the specific circumstances, obtain appropriate information to advise on the use of a method of computer monitoring that is as narrow, time-limited, and non-invasive as is appropriate to carry out the request.

**Legal review:** When a request for computer monitoring is made by a party other than an outside law enforcement or national security authority or the HHS Inspector General, the Chief Counsel will determine whether the monitoring is legally supportable and will notify the CIO, the COO, and the Commissioner or her designee, of these conclusions, including any recommended limits or boundaries. In evaluating the monitoring, the Chief Counsel shall consider whether the proposed monitoring is consistent with all applicable legal requirements, including the Whistleblower Protection Act.

In addition, the Chief Counsel shall inform the parties to whom information derived from monitoring is to be made available that such information may not be used in violation of the

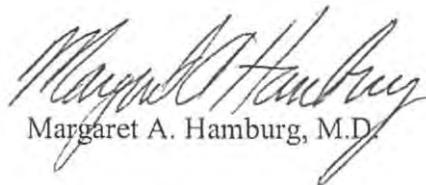
---

<sup>4</sup> Monitoring initiated at the request of outside law enforcement or national security authorities or the HHS Inspector General raises issues that warrant additional consideration on a Department-wide basis. These are expected to be addressed by the additional HHS reviews referenced elsewhere in this document.

Whistleblower Protection Act and related protections. The Chief Counsel will advise other components of FDA on implementing these protections effectively.

**Periodic review of monitoring:** The CIO shall review any computer monitoring on a monthly basis and, in consultation with the individual who authorized the monitoring, assess whether it remains justified or must be discontinued. A decision to continue monitoring shall be explained and documented in writing by the CIO, who shall report monthly to (1) the Commissioner or her delegate, (2) the COO, and (3) the Chief Counsel, regarding the status of any on-going monitoring.

**Special circumstances:** The CIO and Chief Counsel may make recommendations to the Commissioner for additional procedures, if necessary, to address specific circumstances not addressed in this memorandum.



Margaret A. Hamburg, M.D.



**STAFF MANUAL GUIDE 3252.XX**  
GENERAL ADMINISTRATION  
EFFECTIVE DATE: 09/26/2013

FOOD AND DRUG ADMINISTRATION  
INFORMATION RESOURCES MANAGEMENT – INFORMATION TECHNOLOGY  
SECURITY  
OPERATIONAL CONTROL POLICIES

**MONITORING OF USE OF HHS/FDA IT RESOURCES**

**1. PURPOSE.**

This Staff Manual Guide establishes interim policies and procedures that will strengthen the Food and Drug Administration's (FDA) ability to effectively document, analyze, authorize, and manage requests to monitor use of Department of Health and Human Services (HHS or Department) and FDA information technology (IT) systems and resources.

**2. SCOPE.**

This interim policy:

- Applies to all individuals (including, but not limited to current and former civilian government employees, contractors, local or foreign government exchange program participants, Commissioned Corps personnel, guest researchers, visiting scientists, fellows and interns), provided access to HHS/FDA IT systems and resources;
- Covers real-time or contemporaneous observation, prospective monitoring (e.g., using monitoring or keystroke capture software), and retrospective review and analyses (e.g., of e-mail sent or received, or of computer hard-drive contents) targeting an individual;
- Does not apply to computer incident response monitoring of systems relating to national security or the Federal Information Security Management Act of 2002 (FISMA) that perform general system and network monitoring, or examinations of computers for malware;
- Does not apply to any review and analysis requested or consented to by the individual(s) being monitored;
- Does not apply to retrospective searches for documents in response to valid information requests in the context of litigation, Congressional oversight, Freedom of Information Act

(FOIA) requests, and investigations by the Government Accountability Office (GAO) and the Office of Special Counsel;

- This interim policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in place as of this interim policy's effective date; and
- Excludes routine IT equipment examinations. Any unintended discoveries of problematic content and resulting follow-up actions are not subject to this interim policy, although follow-up actions that involve computer monitoring are subject to this interim policy.

### 3. BACKGROUND.

FDA is required to protect vast quantities of sensitive information including, but not limited to, confidential commercial and financial information, trade secrets, protected healthcare information, and classified information. The Department of Health and Human Services (HHS) *Policy for Information Systems Security and Privacy (IS2P)*,<sup>1</sup> requires the use of a warning banner on all Department IT systems. The warning banner must state that, by accessing an HHS/FDA IT system,<sup>2</sup> (e.g., logging onto a Department computer or network), the employee consents to having no reasonable expectation of privacy regarding any communication or data transiting or stored on any HHS/FDA IT system, and the employee understands that, at any time, the Department may monitor the use of Agency IT resources for lawful government purposes. While the warning banner gives FDA the authority to monitor employee use of Agency IT resources, FDA must carry out computer monitoring in a manner that recognizes employee interests and relevant legal protections. FDA will comply with all applicable laws, including but not limited to the Privacy Act of 1974, the privacy provisions of the E-Government Act of 2002, Whistleblower Protection Enhancement Act of 2012, and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts.

### 4. REFERENCES.

HHS *Policy for Monitoring Employee Use of HHS IT Resources*, dated June 26, 2013  
FDA Memorandum, *Monitoring of FDA Personnel Work Computers*, dated September 24, 2012  
HHS IRM Policy for Personal Use of Information Technology Resources dated February 17, 2006  
HHS *Policy for Information Systems Security and Privacy*, dated July 7, 2011  
NIST SP 800-61, Computer Security Incident Handling Guide, dated March 2008  
NIST SP 800-86, Guide to Integrating Forensic Techniques - Incident Response, August 2006

---

<sup>1</sup> Available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>

<sup>2</sup> According to the warning banner, an HHS IT system includes "(1) the computer being accessed, (2) the computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network."

Presidential Policy Directive/PPD-19, *Protecting Whistleblowers with Access to Classified Information*, dated, June 26, 2013

## **5. INTERIM POLICY.**

### **5.1. BASIS FOR COMPUTER MONITORING.**

Computer monitoring may be authorized only for the following reasons:

- a. A written request by OIG, OSSI or an outside law enforcement authority (e.g., FBI, DHS);
- b. Where reasonable grounds exist to believe that the individual to be monitored may be responsible for the unauthorized disclosure of legally protected information (e.g., confidential commercial information or Privacy Act-protected information); or
- c. Where reasonable grounds exist to believe that the individual to be monitored may have violated applicable law, regulation or written HHS or FDA policy.

### **5.2 EXPRESS WRITTEN AUTHORIZATION FOR COMPUTER MONITORING.**

No agency official, including the Chief Information Officer (CIO), may conduct computer monitoring without prior written authorization by one of the following officials:

- FDA Commissioner
- FDA Deputy Commissioner
- FDA Chief Operating Officer

The authority identified herein may not be (re)delegated below the office of Chief Operating Officer. All requests to initiate monitoring must be in writing and shall include an explanation of how the monitoring will be conducted, by what method the information collected during monitoring will be controlled and protected, and a listing of individuals who will be provided access to the information gathered through monitoring. Except for monitoring requested by outside law enforcement authority or the OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. The requesting organization shall document the basis for any request for computer monitoring.

### **5.3 REVIEW COMMITTEE.**

A Review Committee shall be established as described below and as further set forth in implementing procedures. This Review Committee shall consist of a representative from the Office of the Chief Counsel, a representative from the Office of Information Management with Systems Administration expertise, and a representative from the Office of Human Resources

with Human Capital expertise. The Review Committee may draw on additional expertise, as needed.

For designated requests for monitoring, the Review Committee shall review such requests and recommend to an authorizing official specified in 5.2 above, that the official authorize or not authorize a specific request. For other requests, the Review Committee will not ordinarily recommend authorization or non-authorization, although it may at its discretion put a request on hold or make a recommendation concerning authorization to an FDA authorizing official as specified in 5.2 above.

The Review Committee shall develop, as soon as practicable, procedures by which it will review and receive notification of requests for computer monitoring and, if appropriate, explain how such requests are to be submitted and documented. The Review Committee's procedures should ensure that the Committee promptly and efficiently reviews requests for computer monitoring that require a Committee recommendation to an agency authorizing official or which require that the Review Committee be notified of such requests.

In developing implementing procedures, the Review Committee should consider the following framework for review, authorization, and notification of requests for computer monitoring:

- a. Requests from outside law enforcement: The Review Committee should be notified of requests from outside law enforcement for which a Memorandum of Understanding (MOU) or similar written agreement is in effect. Provided such an MOU or similar written agreement is in effect (see 5.4 below), the Review Committee will not ordinarily make a recommendation concerning such requests to an FDA authorizing official. If an MOU or similar written agreement is not in effect, all such requests should be provided to the Review Committee for review and recommendation.
- b. Requests from OIG: The Review Committee should be notified of requests from OIG.
- c. Requests from sources other than outside law enforcement/OIG for prospective monitoring should be provided to the Review Committee for review and recommendation to an authorizing official.
- d. Requests from sources other than outside law enforcement/OIG for retrospective monitoring should, when implementing procedures have been developed, be provided to the Review Committee for review and recommendation, or notification and appropriate action.

#### **5.4 MONITORING REQUESTS FROM OIG AND OUTSIDE LAW ENFORCEMENT.**

Computer monitoring may be requested by outside law enforcement authorities (e.g., Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS))<sup>3</sup> or the HHS Office of Inspector General (OIG). All requests from outside law enforcement agencies must be coordinated through the OIG, except for requests relating to national security or non-criminal insider threat matters, which must be coordinated with the Office of Security and Strategic Information (OSSI) and/or the FDA Security Liaison Officer/Insider Threat Coordinator. Such external computer monitoring requests may be subject to different standards partly because they are covered by the internal controls of the requesting agency or judicial process.

If the monitoring is requested by outside law enforcement authorities, a Memorandum of Understanding (MOU) or similar written agreement may be developed with outside law enforcement as a precondition for approving computer monitoring requests from these organizations.

Such an MOU or similar written agreement shall include the following:

- a. The title and organizational component of the person(s) authorized to request monitoring on behalf of the law enforcement agency;
- b. Documentation of the source of the official request, demonstrating approval by an official of the governmental entity that has the authority to request the initiation of such monitoring (e.g., a subpoena (administrative or grand jury)), warrant or national security letter (NSL), or other acceptable documented request (e.g., a written administrative request that meets the HIPAA Privacy Rule's requirements for certain disclosures to law enforcement agencies);
- c. Any restrictions applicable to the handling and disclosure of confidential information that may be produced by the computer monitoring; and
- d. Other items consistent with this memorandum, including the handling of sensitive communications.

#### **5.5 SCOPE OF COMPUTER MONITORING.**

Requests for computer monitoring shall be narrowly tailored in time, scope, and degree of monitoring. All requests to monitor shall identify the least invasive approach to accomplish the monitoring objectives. When reviewing requests for monitoring, authorizing officials shall also consider whether there are alternative information-gathering methods available (in lieu of monitoring) that can be utilized to address the potential risk, without jeopardizing the agency's objectives. When the monitoring request originates from OIG or outside law enforcement,

---

<sup>3</sup> For the purposes of this interim policy, the term "law enforcement authority" includes national security and intelligence agencies of the U.S. Government.

the authorizing official will grant appropriate deference to requests made in accordance with this memorandum.

## **5.6 DOCUMENTATION.**

The written authorization for computer monitoring must describe the reason for the monitoring. If the monitoring is initiated at the request of outside law enforcement, the authorization must document that the request was approved by an official of the governmental entity that has the authority to request the initiation of such monitoring.

Except for computer monitoring initiated at the request of an outside law enforcement authority or OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. Requests for such monitoring must include: an explanation of how the monitoring will be conducted, by what means the information collected during monitoring will be controlled and protected, and, a listing of individuals who will be provided access to the resultant monitoring information.

A record of all requests for monitoring shall be maintained by the FDA COO, along with any other summary results or documentation produced during the period of monitoring. The record also shall reflect the scope of the monitoring. All information collected from monitoring and maintained by the FDA COO must be controlled and protected, with distribution limited to the individuals identified in the request for monitoring and other individuals specifically designated by the COO as having a specific need to know such information.

## **5.7. LIMITING THE TIME, SCOPE AND INVASIVENESS OF MONITORING.**

The FDA COO will authorize computer monitoring that is appropriately narrow in scope, time-limited, and takes the least invasive approach to accomplish monitoring objectives. The COO, in reviewing requests for computer monitoring, must also consider whether there are alternative information-gathering methods that FDA can utilize to address the concern in lieu of monitoring. When the computer monitoring request originates from OIG or outside law enforcement, the COO authorizing the monitoring will grant appropriate deference to a request made in accordance with this interim policy.

## **5.8. SENSITIVE COMMUNICATIONS.**

No computer monitoring authorized or conducted may target communications with law enforcement entities, the Office of Special Counsel, members of Congress or their staff, employee union officials, or private attorneys. If such communications are inadvertently collected or inadvertently identified from more general searches, they may not be shared with a

non-law enforcement party who requested the monitoring, or anyone else, without express written authorization from OGC and other appropriate HHS and FDA official(s).

#### **5.9. PERIODIC REVIEW OF MONITORING.**

The COO shall review all computer monitoring on a monthly basis and, in consultation with the party who requested the monitoring (e.g., OCI), assess whether it remains justified or must be discontinued. The COO shall consider if the decision for ongoing computer monitoring should be reviewed by OGC. A decision to continue monitoring shall be documented in writing by the COO, who shall report at least monthly, to the Commissioner regarding the status of any ongoing monitoring.

#### **5.10. LEGAL REVIEW.**

Review by the FDA Office of the Chief Counsel of a request for computer monitoring will include, as necessary, consultation with other Divisions of HHS Office of the General Counsel, such as the General Law Division, especially concerning legal requirements such as the Whistleblower Protection Act and the HIPAA Privacy and Security Rule, about which other OGC Divisions have expertise.

#### **5.11 SPECIAL CIRCUMSTANCES.**

The authorizing official and Chief Counsel may make recommendations to the Commissioner for additional procedures, if necessary, to address specific circumstances not addressed in this Staff Manual Guide. Policies and procedures that deviate from the elements of the HHS Memorandum may not be implemented without the written concurrence of the HHS COO in consultation with the OGC.

### **6. ROLES AND RESPONSIBILITIES.**

**FDA Chief Counsel.** Provides legal review and advice regarding requests for, and implementation of, computer monitoring of HHS IT systems and resources. OCC will consult with HHS OGC as needed.

**FDA Chief Operating Officer (COO).** The COO Provides executive direction, leadership, coordination, and guidance for the overall day-to-day administrative operations of the FDA ensuring the timely and effective implementation and high quality delivery of services across the Food and Drug Administration (FDA). The COO will coordinate with the Office of Chief Counsel, the Chief Information Officer, Office of Criminal Investigation (OCI), law enforcement and other authorities on actions and activities involving monitoring of use of IT Resources.

**FDA Chief Information Officer (CIO).** The CIO in the Office of Information Management (OIM) is responsible for executing monitoring as authorized by the Commissioner and COO

following consultation with Chief Counsel. The CIO provides the overall policy, guidance and general oversight of FDA's electronic records and for establishing and implementing the agency incident response plan for responding to the detection of adverse events involving FDA information systems.

**FDA Chief Information Security Officer (CISO).** The FDA CISO is responsible for the establishment and management of the FDA incident response process. The FDA CISO serves as an FDA focal point for incident reporting and subsequent resolution. The CISO provides advice and assistance to Agency managers and other organizational personnel concerning incident response activities.

**FDA Computer Security Incident Response Team (CSIRT).** Headed by the CSIRT Lead, the Incident Response (IR) Team will conduct computing monitoring, forensic capabilities and techniques in accordance with established NIST Standards. The CSIRT provides centralized monitoring, tracking, analysis, insider threat detection, reporting, notification, and coordination of computer security incidents and to report the finding with the appropriate officials in support of law enforcement and national security officials.

## 7. DEFINITIONS.

**Employee** - All individuals (e.g., including, but not limited to current and former civilian government employees, contactors, local or foreign government exchange program participants, Commissioned Corp personnel, guest researchers, visiting scientists, fellows and interns), provided access to Department of Health and Human Services, Food and Drug Administration IT systems and resources.

**IT System** - Includes (1) the computer or electronic device being accessed, (2) the computer network (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.

**Accessing an HHS/FDA System** - e.g., logging on to a government or contractor furnished computer, laptop, Blackberry, iPad, scanner or other electronic device or logging on to the FDA network via local or remote use.

**IT Resources** - Includes but is not limited to: computers and related peripheral equipment and software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to internet services, e-mail and, for the purposes of this policy, office supplies. It includes data stored in or transported by such resources for HHS/FDA purposes.

**Outside Law Enforcement Authority** - Includes national security and intelligence agencies of the United States.

**Passive Monitoring/Computer Incident Response Monitoring** - The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

A handwritten signature in black ink that reads "Walter S. Harris". The signature is written in a cursive style with a large initial "W".

Date: 9/26/13

---

Walter S. Harris, MBA, PMP  
Deputy Commissioner for Operations  
Chief Operating Officer

DARRELL E. ISSA, CALIFORNIA  
CHAIRMAN

ONE HUNDRED TWELFTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND  
RANKING MINORITY MEMBER

DAN BURTON, INDIANA  
JOHN L. MICA, FLORIDA  
TODD RUSSELL PLATTS, PENNSYLVANIA  
MICHAEL R. TURNER, OHIO  
PATRICK MCHENRY, NORTH CAROLINA  
JIM JORDAN, OHIO  
JASON CHAFFETZ, UTAH  
CONNIE MACK, FLORIDA  
TIM WALBERG, MICHIGAN  
JAMES LANKFORD, OKLAHOMA  
JUSTIN AMASH, MICHIGAN  
ANN MARIE BUERKLE, NEW YORK  
PAUL A. GOSAR, D.D.S., ARIZONA  
RAUL R. LABRADOR, IDAHO  
PATRICK MEEHAN, PENNSYLVANIA  
SCOTT DESJARLAIS, M.D., TENNESSEE  
JOE WALSH, ILLINOIS  
TREY GOWDY, SOUTH CAROLINA  
DENNIS A. ROSS, FLORIDA  
FRANK C. GUINTA, NEW HAMPSHIRE  
BLAKE FARENTHOLD, TEXAS  
MIKE KELLY, PENNSYLVANIA

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-6074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

EDOLPHUS TOWNS, NEW YORK  
CAROLYN B. MALONEY, NEW YORK  
ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA  
DENNIS J. KUCINICH, OHIO  
JOHN F. TIERNEY, MASSACHUSETTS  
WM. LACY CLAY, MISSOURI  
STEPHEN F. LYNCH, MASSACHUSETTS  
JIM COOPER, TENNESSEE  
GERALD E. CONNOLLY, VIRGINIA  
MIKE OUGLEY, ILLINOIS  
DANNY K. DAVIS, ILLINOIS  
BRUCE L. BRALEY, IOWA  
PETER WELCH, VERMONT  
JOHN A. YARMUTH, KENTUCKY  
CHRISTOPHER S. MURPHY, CONNECTICUT  
JACKIE SPEIER, CALIFORNIA

LAWRENCE J. BRADY  
STAFF DIRECTOR

May 9, 2012

The Honorable Richard A. Lidinsky, Jr.  
Chairman  
Federal Maritime Commission  
800 North Capitol Street, NW  
Washington, DC 20573

Dear Mr. Chairman Lidinsky:

It has come to my attention that the Federal Maritime Commission (FMC) may be an agency in crisis. Commission insiders allege that the politicization of the Commission's core functions and administrative decisions has contributed to a climate of fear and intimidation among agency managers and staff. As you know, the Office of Special Counsel has opened an investigation into these allegations.

The effect on the staff has been measurable. According to the Partnership for Public Service, which produces the respected federal employee satisfaction survey *The Best Places to Work in the Federal Government*, in 2011 the FMC suffered the largest drop in employee satisfaction of any agency in government.<sup>1</sup> The Committee observed a similar chilling effect on the staff when the Chairman of the Nuclear Regulatory Commission politicized the agency and bullied career staff. The Committee treats allegations of politicization of independent regulatory agencies very seriously because, if true, they can undermine the performance of an agency's mission. The purpose of this letter is to request documents and information to better understand the allegations concerning the Federal Maritime Commission.

The allegations center on your treatment of staff who objected to banning owner-operator truck drivers from providing services at the Port of Los Angeles (POLA). Prior to your being named Chairman in September 2009, the FMC was involved in litigation concerning the POLA Clean Truck Program (CTP), which was intended to reduce air pollution at the port.<sup>2</sup> The FMC opposed one provision of the CTP, unrelated to air pollution, which would have effectively banned independent owner-operator truck drivers, who provide the vast majority of port drayage services, from working at POLA.<sup>3</sup> Instead, under POLA's proposal, only trucking companies utilizing employee-drivers, who are subject to unionization, would be allowed to work at the

<sup>1</sup> THE BEST PLACES TO WORK IN THE FEDERAL GOVERNMENT (2011), <http://bestplacestowork.org/BPTW/rankings/overall/small>.

<sup>2</sup> Ronald D. White, *Agency Objects to Clean Truck Program*, L.A. TIMES, Oct. 30, 2008.

<sup>3</sup> S. Calif. Port Truck Plan Supporters Warn Current Version Will Fail, SHIPPERS' NEWSWIRE, July 5, 2007.

port. However, FMC economists Roy Pearson and Robert Blair testified in federal court that this provision would reduce competition and “unreasonably increase transportation costs,” and was “not in any way critical to sustaining the CTP’s environmental and public health benefits.”<sup>4</sup>

Labor unions,<sup>5</sup> environmental groups,<sup>6</sup> and “green jobs” advocacy organizations decried FMC’s opposition to the employee-driver mandate, as set forth by Pearson and Blair in their court testimony.<sup>7</sup> The Natural Resources Defense Council filed a Freedom of Information Act request for FMC documents in an attempt to prove that “external influences” may have precipitated the agency’s “rabid attacks and scrutiny” of the employee-driver mandate.<sup>8</sup> According to information received by the Committee, the nonpartisan Office of the Secretary and the General Counsel’s office – not the Chairman’s Office – typically handle FOIA requests.

One of your first acts as Chairman was to insert yourself into the nonpartisan FOIA process by ordering that six boxes of Blair’s work papers concerning CTP be sent to your office for review. You made this request despite the fact that these documents were the subject of ongoing litigation between the FMC and the Natural Resources Defense Council.

The Committee has learned that Blair and Pearson may have faced retaliation for testifying in opposition to the employee-driver mandate in federal court. According to information received by the Committee, in October 2009 you told Blair and Pearson’s supervisor Austin Schmitt to “keep an eye on” them. You further advised their supervisor that Blair and Pearson did not reflect well on the agency, and that Blair, who had worked for a time at the World Shipping Council, an association representing ocean carriers, was a “spy for the carriers” inside the agency. Furthermore, you allegedly told Schmitt that you regretted not having sought permission from OPM to fire Blair and Pearson. In another instance, following a presentation Pearson gave to Commissioners and staff, you stated:

I’ve had several complaints concerning [Pearson’s] ‘performance’ at meeting yesterday – which fell somewhere between a red brick poly in Liverpool or a too-clever-by-half over the hill vaudevillian who once read a book. He took way too much time on a very busy day, too obtuse charts and his never-ending arrogant sneer toward the bench. Who vetted his

---

<sup>4</sup> Decl. of Dr. Roy J. Pearson in Supp. of Pl.’s Mot. for Prelim. Inj., at 5, 6-7, Fed. Mar. Comm’n v. City of Los Angeles, et al., No. 08-1895 (D.D.C. Nov. 17, 2008).

<sup>5</sup> Press Release, International Brotherhood of Teamsters, Environmental-Led Port Coalition Praises President Obama’s Pick of Joseph Brennan to Lead FMC (June 9, 2009), <http://www.teamster.org/content/environmental-led-port-coalition-praises-president-obamas-pick-joseph-brennan-lead-fmc>.

<sup>6</sup> David Pettit, *A Truckload of Hypocrisy*, NATURAL RESOURCES DEFENSE COUNCIL, Sept. 17, 2008, [http://switchboard.nrdc.org/blogs/dpettit/a\\_truckload\\_of\\_hypocrisy.html](http://switchboard.nrdc.org/blogs/dpettit/a_truckload_of_hypocrisy.html).

<sup>7</sup> Press Release, Coalition for Clean & Safe Ports, National “Blue-Green” Coalition Applauds Key Obama Appointee’s Inaugural Earth Day Award to LA Clean Truck Program (April 21, 2010), <http://cleanandsafeports.org/resources-for-the-media/press-releases/national-blue-green-coalition-applauds-key-obama-appointees-inaugural-earth-day-award-to-la-clean-truck-program/>.

<sup>8</sup> NRDC, “The Federal Maritime Commission Needs a Lesson in Transparency,” May 19, 2009, *available at* [http://switchboard.nrdc.org/blogs/amartinez/the\\_federal\\_maritime\\_commission.html](http://switchboard.nrdc.org/blogs/amartinez/the_federal_maritime_commission.html).

performance time? I will decide in the future what time he has. Take this up with his supervisor, RL.<sup>9</sup>

The Committee has learned that Schmitt may also have faced retaliation for defending Blair and Pearson. On September 20, 2010, Schmitt, in his capacity as Blair and Pearson's direct supervisor, gave them an adjectival performance rating of "Outstanding" and recommended they each receive an annual performance award of 3 percent of base salary, the minimum amount commensurate with an "Outstanding" rating under established FMC policy.<sup>10</sup> According to documents reviewed by the Committee, this would have equated to awards of roughly \$3,800 to \$4,200, respectively.<sup>11</sup>

In spite of these ratings, you informed Schmitt through the Managing Director that you wanted Blair and Pearson to receive no more than \$200 each, despite the fact that both their direct supervisor and FMC Commissioner Rebecca Dye had lauded their work performance as "outstanding."<sup>12</sup> After Schmitt protested that this would violate agency policy, you agreed to a 2 percent award for Blair and Pearson. You refused to put your rationale for rejecting the reviewing supervisor's recommendation in writing, despite the fact that doing so is also required by established agency policy.<sup>13</sup>

According to documents obtained by the Committee, on the same day that Schmitt refused to arbitrarily lower his recommended performance award for Blair and Pearson without written explanation from your office, you informed Schmitt that his department would be subjected to a "management survey."<sup>14</sup> One of the staffers tasked to conduct this "management survey" later resigned, in part because he believed his task was to conduct a biased investigation designed to produce predetermined conclusions and damaging information about Schmitt and others.

In addition to adverse personnel decisions taken against them, the Committee has learned that agency management subjected Schmitt, Blair and Pearson, along with at least three other FMC employees, to covert surveillance of their computers and e-mails by means of software called Spector 360. According to the company's website, this software captures all the workstation activity of a monitored employee.<sup>15</sup> The Committee has learned that the Inspector General for the FMC expressed concern about whether the agency's use of this software violated federal privacy regulations and requested that agency management stop using it in January 2012.

---

<sup>9</sup> E-mail from Richard A. Lidinsky, Chairman, Federal Maritime Commission, to Ronald Murphy, Managing Director, Federal Maritime Commission (July 14, 2011).

<sup>10</sup> FEDERAL MARITIME COMMISSION, RECOMMENDATION FOR PERFORMANCE OR INCENTIVE AWARD (Sept. 20, 2010).

<sup>11</sup> FEDERAL MARITIME COMMISSION, *supra* note 10.

<sup>12</sup> Memoranda from Rebecca Dye, Commissioner, Federal Maritime Commission to Austin Schmitt, Director, Bureau of Trade Analysis (Sept. 13, 2010) (on file with author).

<sup>13</sup> FEDERAL MARITIME COMMISSION, *supra* note 11, § (f)(7).

<sup>14</sup> Memorandum from Ronald D. Murphy, Managing Director, Federal Maritime Commission to Austin Schmitt, Director, Bureau of Trade Analysis (Sept. 22, 2010).

<sup>15</sup> SpectorSoft, Computer & Internet Monitoring Software, <http://www.spector360.com/> (last visited May 8, 2012).

Despite this admonition, it appears agency management continued using Spector 360 against the advice of the Inspector General.

The Committee is also concerned about misuse of taxpayer funds. For example, according to information we have received, the FMC procured an official car and chauffer used mostly to drive you from FMC headquarters to Union Station, a distance of approximately three blocks.

To assist the Committee's investigation of this matter, please provide the following documents and information as soon as possible, but by no later than May 22, 2012, at noon:

1. All documents and communications, from July 1, 2009, to the present, between and among Richard A. Lidinsky, Ronald D. Murphy and the following organizations/individuals:
  - a. Natural Resources Defense Council;
  - b. International Brotherhood of Teamsters;
  - c. International Longshoremen's Association;
  - d. International Longshore and Warehouse Union;
  - e. Coalition for Clean & Safe Ports;
  - f. Change to Win;
  - g. Office of the Honorable Antonio Villaraigosa, Mayor of Los Angeles;
  - h. Office of Geraldine Knatz, Executive Director, Port of Los Angeles;
  - i. Office of the Honorable Nancy Pelosi; and
  - j. Executive Office of the President.
  
2. All documents and communications, from July 1, 2009, to the present, referring or relating to Austin Schmitt, Roy Pearson, Robert Blair, Edward Anthony, Spector 360 software, the *Survey of Bureau of Trade Analysis Programs* (Aug. 22, 2011), the Natural Resources Defense Council FOIA request, the Port of Los Angeles Clean Truck Program, and the Chairman's Inaugural Earth Day Award, between and among Richard A. Lidinsky, Ronald D. Murphy and the following individuals:
  - a. Rebecca A. Fenneman;
  - b. Adam R. Trzeciak;
  - c. Laura Mayberry;
  - d. Jerome Johnson;
  - e. Michael H. Kilby;
  - f. David Story; and
  - g. Anthony Haywood.
  
3. A complete accounting of the agency's purchase and use of Spector 360 software, including the total amount of agency funds expended, the agency employees subjected to monitoring, the justification for monitoring them, whether the FMC Inspector General requested that the agency stop using Spector 360 to monitor certain employees, and whether the agency immediately complied with that directive.

4. A complete accounting of the agency's procurement of a vehicle for the purpose of transporting commissioners and agency employees, including:
  - a. The year, make and model of the vehicle;
  - b. The total amount spent on the vehicle, including any costs involved in securing garage space for the vehicle;
  - c. The salary of any individual whose job description includes driving the vehicle; and
  - d. All records describing the use of the vehicle including origins, destinations, frequency of use, and passengers.
5. A complete accounting of the agency's purchase of any decorative or commemorative items such as paintings, sculptures, works of art, furniture, or coins on behalf of the Office of the Chairman since September 11, 2009, including the total amount spent and the method of payment.
6. A complete accounting of the agency's 50th Anniversary Party, including total funds expended and a break-down of funds expended by category.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request.

If you have any questions about these requests, please contact Brien Beattie or Jonathan Skladany of the Committee staff at (202) 225-5074. Thank you for your attention to this important matter.

Sincerely,



Darrell Issa  
Chairman

Attachment

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

ONE HUNDRED TWELFTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM  
2157 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6143

Majority (202) 225-5074  
Minority (202) 225-5051

**Responding to Committee Document Requests**

1. In complying with this request, you should produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
  - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
  - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.
7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when they were requested.
8. When you produce documents, you should identify the paragraph in the Committee's request to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full, compliance shall be made to the extent possible and shall include an explanation of why full compliance is not possible.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you should produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. The time period covered by this request is included in the attached request. To the extent a time period is not specified, produce relevant documents from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.
19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email, regular mail, telexes, releases, or otherwise.
3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might

otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.
5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.