

**LIMITLESS SURVEILLANCE AT THE FDA: PRO-
TECTING THE RIGHTS OF FEDERAL WHISTLE-
BLOWERS**

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

FEBRUARY 26, 2014

Serial No. 113-88

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: <http://www.fdsys.gov>
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

87-176 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida	ELLJAH E. CUMMINGS, Maryland, <i>Ranking</i>
MICHAEL R. TURNER, Ohio	<i>Minority Member</i>
JOHN J. DUNCAN, JR., Tennessee	CAROLYN B. MALONEY, New York
PATRICK T. McHENRY, North Carolina	ELEANOR HOLMES NORTON, District of
JIM JORDAN, Ohio	Columbia
JASON CHAFFETZ, Utah	JOHN F. TIERNEY, Massachusetts
TIM WALBERG, Michigan	WM. LACY CLAY, Missouri
JAMES LANKFORD, Oklahoma	STEPHEN F. LYNCH, Massachusetts
JUSTIN AMASH, Michigan	JIM COOPER, Tennessee
PAUL A. GOSAR, Arizona	GERALD E. CONNOLLY, Virginia
PATRICK MEEHAN, Pennsylvania	JACKIE SPEIER, California
SCOTT DESJARLAIS, Tennessee	MATTHEW A. CARTWRIGHT, Pennsylvania
TREY GOWDY, South Carolina	TAMMY DUCKWORTH, Illinois
BLAKE FARENTHOLD, Texas	ROBIN L. KELLY, Illinois
DOC HASTINGS, Washington	DANNY K. DAVIS, Illinois
CYNTHIA M. LUMMIS, Wyoming	PETER WELCH, Vermont
ROB WOODALL, Georgia	TONY CARDENAS, California
THOMAS MASSIE, Kentucky	STEVEN A. HORSFORD, Nevada
DOUG COLLINS, Georgia	MICHELE LUJAN GRISHAM, New Mexico
MARK MEADOWS, North Carolina	<i>Vacancy</i>
KERRY L. BENTIVOLIO, Michigan	
RON DeSANTIS, Florida	

LAWRENCE J. BRADY, *Staff Director*

JOHN D. CUADERES, *Deputy Staff Director*

STEPHEN CASTOR, *General Counsel*

LINDA A. GOOD, *Chief Clerk*

DAVID RAPALLO, *Minority Staff Director*

CONTENTS

Hearing held on February 26, 2014	Page 1
WITNESSES	
The Hon. Charles E. Grassley, A U.S. Senator from the State of Iowa	
Oral Statement	9
Written Statement	13
Mr. Walter Harris, Chief Operating Officer and Acting Chief Information Officer, U.S. Food and Drug Administration, Accompanied by Jeffrey Shuren, M.D., Director, Center for Devices and Radiological Health, U.S. Food and Drug Administration, and Ruth McKee, Associate Director for Management, Center for Devices and Radiologic Health, U.S. Food and Drug Administration	
Oral Statement	21
Written Statement	24
Ms. Angela Canterbury, Director of Public Safety, Project on Government Oversight	
APPENDIX	
HHS Office of IG Report, Submitted by Rep. Issa	88
Joint Staff Report, Submitted by Rep. Issa	119
Letter to Rep. Cummings from Rep. Issa, Submitted by Rep. Issa	271

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

Wednesday, February 26, 2014

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 10:00 a.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Turner, Duncan, Jordan, Walberg, Lankford, Amash, Farenthold, Woodall, Massie, Collins, Meadows, Bentivolio, Cummings, Maloney, Lynch, Connolly, Speier, Kelly, and Lujan Grisham.

Staff Present: Alexia Armstrong, Legislative Assistant; Molly Boyd, Deputy General Counsel and Parliamentarian; Lawrence J. Brady, Staff Director; Ashley H. Callen, Deputy Chief Counsel for Investigations; Sharon Casey, Senior Assistant Clerk; John Cuaderes, Deputy Staff Director; Lamar Echols, Counsel; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Caroline Ingram, Professional Staff Member; Mark D. Marin, Deputy Staff Director for Oversight; Ashok M. Pinto, Chief Counsel, Investigations; Krista Boyd, Minority Deputy Director of Legislation/Counsel; Aryele Bradford, Minority Press Secretary; Jennifer Hoffman, Minority Communications Director; Elisa LaNier, Minority Director of Operations; Una Lee, Minority Counsel; Juan McCullum, Minority Clerk; and Dave Rapallo, Minority Staff Director.

Chairman ISSA. The committee will come to order.

The Oversight Committee's mission statement is that we exist to secure two fundamental principles: First, Americans have a right to know that the money Washington takes from them is well spent; and, second, Americans deserve an efficient, effective government that works for them.

Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn responsibility is to hold government accountable to taxpayers, because taxpayers have a right to know what they get from their government.

It is our job to work tirelessly in partnership with citizen watchdogs and whistleblowers to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

Before I deliver my opening statement, because we have Senator Grassley here, I am going to ask unanimous consent that the IG report released last night entitled Department of Health and

Human Services IG Report, "Review of the Food and Drug Administration's Computer Monitoring of Certain Employees in Its Center for Devices and Radiological Health" be placed in the record. Without objection, so ordered.

Additionally, I ask that the joint staff report entitled "Limitless Surveillance at the FDA: Protecting the Rights of Federal Whistleblowers," be placed in the record.

Mr. CUMMINGS. Mr. Chairman?

Chairman ISSA. Yes.

Mr. CUMMINGS. I have no objections, but I just want to make sure it is clear that that is the staff report of the Republicans. Is that right?

Chairman ISSA. It is a joint report of the House and Senate Republicans.

Mr. CUMMINGS. House and Senate. So the Senate Democrats were not involved. In this report, the Senate Democrats—

Chairman ISSA. This report is a result of an investigation in which all your Democrats' staff were in there, but we did not ask for or provide a long comment period to your people. You are entitled to place a minority staff report at your convenience. You have the same information.

Mr. CUMMINGS. We will definitely do that. I just wanted to make it clear on the record.

Chairman ISSA. Absolutely.

Without objection, so ordered. They are both in the record.

And I will place my entire opening statement in the record and be brief.

Today's hearing is about a questionable practice at the FDA, one that has been under investigation for over 2 years—or almost 2 years, July of 2012, by the Inspector General, one that we do not consider to be political in any way, shape, or form, or partisan in any way, shape, or form.

We consider it to be questionable, if not despicable, that whistleblowers, a known whistleblower and others, appear to have been targeted for an investigation proactively monitoring, effectively a wiretap on their computers, in order to see if they could get the dirt on employees so that they could take action.

The FDA justified this based on a leak to the New York Times. However, to the best of our investigation, rather than working retrospectively to see if they could discover who had in the past leaked, they began a practice of monitoring computers, one that captured all information, forwarded all information, including, at a minimum, correspondence as whistleblowers with three members of Congress's staff, Senator Grassley's, our staff, and Chris Van Hollen of Maryland.

It does not matter whether it is one or all. It does not matter whether it is a Republican or a Democrat. This committee believes in whistleblowers, encourages whistleblowers, and particularly believes that communications with members of Congress, the other branch, Article 1, are, in fact, off limits to that kind of monitoring.

It appears as though no protections were placed on that, but, rather, this was an attempt at "gotcha." There may have been good reason to be concerned. An investigation into leaks may have been very justified. In this case, we are not questioning whether or not

an investigation should have occurred, but, rather, the tactics and the lack of protection there.

Today we are holding this hearing, and we are pleased to welcome Senator Grassley, whose investigation really kicked this off and whose staff has worked hand in hand, along with the Democratic members of this committee's staff, on hearing all of the witnesses.

I might note, during the period of July 2012, when this began, until now, whistleblowers involved in this have been reticent to go on the record. They have wanted to deliver with as few people hearing what they have to say as possible and then let the facts speak for themselves.

In the purest sense, that is what whistleblowers should do. In the purest sense, we should have an independent investigation that discovers the facts with limited testimonial by the whistleblowers. Their concern when they are reporting, essentially, whistleblower retaliation is certainly understandable.

Neither the IG nor the minority on this committee has had an opportunity to speak to those whistleblowers. I will continue to encourage them to speak to both the IG and minority staff, but it is their decision.

A whistleblower may come to one member of Congress, any one member of Congress, in my opinion, and that member of Congress should proceed on his constitutional or her constitutional responsibility and protect the whistleblower to the greatest extent possible. This committee will also always support that protection.

The misconduct that we are looking at is not just overreach. It mirrors a famous book and movie ripped from the pages of George Orwell's "1984." Constant monitoring of your screens. The only thing that was missing, of course, was a camera looking both ways.

I am here to say that the Federal employees know that every communication they do on government property, on government time, or using government assets, or doing government business is subject to the Federal Government looking at it. There is no expectation of privacy.

But that is not to say that targeting is appropriate. It is not to say that these five scientists' and doctors' concerns are not reasonable. They are.

If there is a reason on behalf of the government to look at the use of government assets, government communication, of course, we expect the Executive Branch to do that.

However, if there is going to be use of products such as Spector 360, a product that captured every 5 seconds the screens of the computers being used and the keystrokes, then, quite frankly, it has to be done for all at every moment and then there have to be rules on how it can be used.

I am not suggesting that. Just the opposite. The Federal workforce is a highly trusted force, and trust is what we depend on. At times, it is clear that that trust is broken and, when it is, there are appropriate remedies.

But until that trust is broken, we depend on a skilled and motivated workforce that believes, as they should, that they are not working for Big Brother, that, in fact, they are trusted in their

roles and not being unreasonably spied on or targeted for disciplinary action.

For that reason, we are holding this hearing today not as just an indictment of the FDA, which I think Senator Grassley will speak to, but as a recognition that all Federal employees need to be protected from an unreasonable activity, which, at least in this chairman's opinion, is part of what went on at the FDA in targeting these five whistleblowers.

Again, I will put the rest of my opening statement in the record. And I yield to the ranking member.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Today we examine two distinct, but related, issues. First, we will review allegations that the FDA employees leaked trade secret and other confidential business information from companies seeking FDA approval of medical device applications.

We will also review allegations by these employees that they were whistleblowers concerned about the safety of these medical devices and that the FDA retaliated against them by monitoring their computers.

Whistleblowers play a critical role in rooting out waste, fraud, and abuse at Federal agencies and making our government more effective and efficient. They sometimes risk their careers. They sometimes risk their reputations to challenge the abuse of power.

Our committee must take every allegation very seriously with regard to retaliation. I have said it before and I will say it again. We must at every point protect our whistleblowers. I am committed to that, and we are all committed to that.

Unfortunately, the majority has taken a traditionally bipartisan issue, something that all committee members should be investigating together, and turned it into another partisan spectacle for which our committee has become well known.

One of the most basic steps that our committee should have taken was to interview the FDA employees who had concerns. I remind all of us that everybody on this side of the aisle and everybody on that side of the aisle represents 700,000 people each, every one of us, the 435 members of our Congress.

As the foundation for a responsible investigation, we should have met with them, asked them questions, learned about their concerns, and given them an opportunity to address evidence that may contradict their accounts.

Instead, despite multiple requests from the Democratic side over the past year, the chairman declined to hold interviews with these employees, although he and Senator Grassley apparently have been communicating with them directly.

These employees were never called in for standard committee interviews. And I heard what the chairman said. But at the same time, as I have said, we need to have an opportunity, just as Senator Grassley has, to talk to these folks, just as the chairman has.

As a result, most committee members have no opportunity to talk to these employees and will not have the benefit of their input as we proceed. Again, we are talking about effectiveness and efficiency. We are talking about transparency with regard to the members of the committee.

The chairman also chose to issue a highly partisan Republican staff report this morning. Just to be clear, this is not an official committee report. It did not follow committee rules for an official committee report. It was not vetted for accuracy by the committee.

Also unfortunate was the timing of today's hearing. Over the past month, the Inspector General was finishing his own investigation and was poised to issue his report on this issue.

Rather than wait a week or two so the committee could hear directly from the IG, the committee rushed to hold today's hearing, apparently trying to beat the IG to the press.

As a matter of fact, the press got the report before we did, their report. It is interesting that we have a situation where the IG was able to complete his report, and he provided it to the committee last night.

Now, let us look at what the IG found, first, "The FDA"—this is the IG—"had reasonable concern that confidential information, including possibly trade secrets and/or CCI, had been disclosed by agency employees without authorization."

Companies that submitted applications had asked the FDA to investigate which employees leaked their trade secret and confidential commercial information in violation of the law.

The IG found, "The FDA had provided notice to its scientists and all other users of the network through a network log-on banner that there was no right to privacy on the FDA computer network and that all data on the network was subject to interception by the FDA."

The committee's investigation has identified no evidence that the FDA monitored employees to retaliate against them. The agency had a reasonable basis for initiating the monitoring, since the disclosure of proprietary information is prohibited by law and subject to criminal penalties.

The IG also found that, regardless of whether the computer monitoring was allowable under the law, the FDA did not have sufficient safeguards to ensure that monitoring would avoid collecting communications with Congress, the Office of Special Counsel, or the IG.

As I close, despite the reasonableness of the FDA's concerns and its explicit warnings that employee computers could be monitored, the IG found that, "The FDA" "should have assessed beforehand and—with the assistance of legal counsel, whether potentially intrusive EnCase and Spector monitoring would be the most appropriate investigative tools and how to ensure that the use of these tools would be consistent with constitutional and statutory limitations on government searches."

The FDA has now implemented new policies that require written authorization from the chief operating officer to initiate monitoring and a legal review of the proposed monitoring by the chief counsel, including a determination that proposed monitoring is consistent with the Whistleblower Protection Act.

Protecting the rights of whistleblowers is an issue we should all be working on together, and our committee has done so in the past. In 2012, this committee passed the Whistleblower Protection Enhancement Act, which was signed into law on November 27, 2012.

This is strong evidence that, when the committee operates on a bipartisan basis, we can accomplish very important and even groundbreaking accomplishments. I hope we can return to that type of bipartisanship in the future. I look forward to hearing from the witnesses.

Mr. Chairman, I thank you for your indulgence.

Chairman ISSA. Of course.

I now ask unanimous consent the letter dated February 25th by me to the ranking member be placed in the record. Without objection, so ordered.

Mr. Cummings, I might note that the IG report which came out at 4:30 last night was preceded by the staff report being given to your staff, which contained substantially all of the same information as the IG report, and we noticed on January 14th the FDA of our plan to have today's hearing.

At that time, we had no expectation that the IG was going to conclude. And, in fact, in a Herculean way, the administration managed to respond to the IG's comments in two days, and the IG managed to get it out last night. We are proud of the fact that that report would not have been in our hands today had we not been scheduling this hearing.

Mr. CUMMINGS. Well, Mr. Chairman, would the gentleman yield?

Chairman ISSA. Of course.

Mr. CUMMINGS. I think the IG and the administration wanted—the administration wanted to get that report out because it felt that it would be significant with regard to any hearing that we might hold.

And so, therefore, those who might have commented from the administration reserved comment so that they could get the report out because we know that all of us have tremendous confidence in the IG.

And I guess, going back to efficiency and effectiveness, that, if we have an IG report, an independent agency that has looked at these things very carefully, it would be nice to have that report before the hearing. To me, that is effectiveness and efficiency.

Chairman ISSA. And the good news is we do have it.

I might note, by the way, that I never spoke to any whistleblower. We can certainly ask Senator Grassley. I never spoke to them directly.

Mr. CUMMINGS. Did your staff?

Chairman ISSA. As you have said so many times, Mr. Cummings, the book "The Speed of Trust" is about trust being earned.

The whistleblowers were unwilling to meet with members of your staff because they did not trust that this would not turn into retaliation. That is through their attorneys. And they are represented by counsel, what we have been told.

So my staff encouraged them and has in no way dissuaded them from talking to your staff, and I openly this morning encourage them once again to come and meet with them.

But, quite frankly, since this hearing is about inappropriate—now determined by the IG to be inappropriate targeting of whistleblowers using questionable tactics, you can understand why the whistleblowers, who, to my knowledge—I do not know, but they may or may not be some of the people targeted here—are reluctant

to be prosecuted, persecuted, and triggered again by an agency that they do not personally believe in.

They do not trust their agency, and they do not trust those who would report back to their agency. That is not my fault. That is not your fault. But that is the reality that the whistleblowers have.

Mr. CUMMINGS. Could we not have brought them in for interviews?

Chairman ISSA. Yes. I could haul in whistleblowers and expose them to the—

Mr. CUMMINGS. We haul in people all the time.

Chairman ISSA. I could expose them to the administration knowing about them and then retaliating against them. I could do that.

But I will protect whistleblowers' right to give us information. Without their testimony, we have independently—and the IG has independently reached the conclusions which we will see today. So I think the record speaks for itself.

Whistleblowers made Senator Grassley and his staff aware of a problem, but independent investigation by the IG and by this committee—bipartisan investigation—have led us to the conclusions we will hear today.

And, by the way, the hearing is not about the leak of information. It is about the unreasonable retaliation. I might caution you that we did not investigate the specifics of the leak of this material. It is certainly a knowledgeable fact. But our investigation began in the retaliation, not in that—

Mr. CUMMINGS. Just one more inquiry.

Chairman ISSA. Of course.

Mr. CUMMINGS. I know Senator Grassley is—

Chairman ISSA. He has been patient, and his time is limited.

Mr. CUMMINGS. Thank you.

This is a question. You know, life is short. And so you just said that you did not look at the allegations made by the whistleblowers. Is that what you are trying to say?

Chairman ISSA. No. The whistleblowers made allegations that led to an investigation. Senator Grassley, I am sure, will cover this. The investigation independently determined what they had said.

We are not relying on their allegations. They are not fact witnesses for purposes of the IG, Senator Grassley's staff, or my staff.

The result of both the pieces of paper, the package you have, are the results of independent—the IG and your staff and my staff and Senator Grassley's staff—interviews. We did not need the whistleblowers except to be aware of a problem.

The investigation is complete and does not need further testimony. In other words, there was no reason to expose the whistleblowers to the possibility of retaliation because their allegations have been confirmed independently.

You believe it, and I believe it, and the IG believes it, that this retaliation that was done against these five people was, in fact, done.

Mr. CUMMINGS. If the gentleman will yield.

Chairman ISSA. Of course.

Mr. CUMMINGS. The only thing I am getting to is that—and Senator Grassley, I am sure, will address this—if there is equipment being used in hospitals that is defective, that people are getting

diseases from, I mean, that's—I mean, we got two issues here. I want to make sure that we deal with that.

Because we can get so caught up in the political stuff that we forget the people who are the victims of some of this, one of which—and I don't know whether it was from equipment, but I just had a constituent to die after giving birth to twins from disease that was contracted in the hospital this week.

So I am trying to figure out will we—are we going—I mean, we got two parts here. We got the whistleblowers. And I think the reason why the whistleblowers bring information to us is so that we can do some reform—remember, that's a part of our title—and try to make sure that the constituents that we serve are safe.

So you are saying that we will not get to that piece of it?

Chairman ISSA. No. Not at all. I am saying that the investigation was as to the retaliation.

Dr. Smith, who was a qualified whistleblower, had deep concerns about the FDA's process and validity of medical devices they certified, and he made allegations that the FDA was not doing their job properly. That's the initial whistleblower activity, which was not disputed.

The leak, justified in the FDA general counsel's mind, which makes me question whether or not these reforms are any good when the general counsel was receiving the information, made them believe that they could monitor five employees prospectively on everything, including their communications with Congressman Van Hollen, Senator Grassley, and my staff. That is what we are researching today.

I am not qualified, quite frankly, to look at the allegations of medical device effectiveness, and I don't believe his initial claim came to our committee on the invalidity of the medical devices.

But Dr. Smith, who is not a witness here today and is not part of it, was a qualified whistleblower. He had complaints, and he was making them.

The investigation was not—supposedly not about his whistleblowing, but he became the target when they said that there had been a leak, which apparently there had.

And I am perfectly happy to have people drift off onto the question of the leak in the New York Times. But what we do know is, although leaks to the New York Times occur all the time, we have whistleblower retaliation in the unreasonable, if you will, activities, in the opinion of the IG and in the opinion of this committee staff report.

And that's what the primary reason for the hearing is, is we do not want to have a chilling effect on potential whistleblowers.

But, more importantly, you and I know that we have to and we had better trust our Federal employees and not be spying on them 24/7, even though we have a right to look at the material on which they work, if necessary.

Mr. CUMMINGS. As I close, let me just say this. You talk about "The Speed of Trust." And I don't want anybody watching this or hearing this to be left with the impression that folks on this side of the aisle, including our staffs, in some kind of way are not protective of whistleblowers. I don't want that getting out into the universe because it's simply not true. I would never say that.

Chairman ISSA. And, Mr. Cummings, I am not asserting that you are not trustworthy. What I am asserting—

Mr. CUMMINGS. And my staff.

Chairman ISSA. —is that the whistleblowers were unwilling to. And I have been corrected on one thing. In 2009, under Chairman Towns, Dr. Smith provided thousands of pages to this committee in support of his whistleblower allegation. So that is really the beginning of Dr. Smith's activity, as far as this committee goes.

And he was a qualified whistleblower, having come to Chairman Towns and this committee with his concerns—and I think other committees—with his concerns about the FDA's activity.

And, again, even though I also serve on Energy and Commerce, I am not claiming that I can understand the details of his allegations.

And I would like, to the greatest extent possible, to caution all Members to primarily look at the question of whether the activities at the FDA, pursuant to their trying to find a leak, crossed a line and interrupted and would have a chilling effect on whistleblowers, which I think is what our committee's primary jurisdiction is.

Mr. CUMMINGS. And, Mr. Chairman, which is my primary concern, also.

Chairman ISSA. Okay. Senator Grassley, you have been incredibly patient. You have heard more testimony than you planned to. And, with that, such time as you may consume.

WITNESS STATEMENTS

STATEMENT OF THE HON. CHARLES E. GRASSLEY, A UNITED STATES SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Before I read, I would like to say a couple things.

Chairman ISSA. Our mics on this side don't amplify as well. They need to be much closer. They are House mics.

Senator GRASSLEY. Two things I would like to say before I read, one, generally about whistleblowing. In 33 years, under both Republicans and Democrats, I found the problem the same, whatever bureaucracy you are talking about. Whistleblowers are about as welcome in a bureaucracy as skunks at a picnic. There is a great deal of peer pressure to go along to get along.

And then, specifically in regard to the FDA, just so everybody knows, we have a Democrat President, but going back to 2003, when I first got involved with whether or not the scientific process was being respected within the FDA and respected scientists coming forward—first was Vioxx and then several things since then—we have found problems with the respect of scientists and the respect of the scientific process within that agency, regardless of who was President.

Thank you, Chairman Issa, for calling this important hearing and for the great work that you and your staff have done. Together, we have conducted a detailed investigation into the FDA aggressive surveillance of whistleblowers.

A group of FDA scientists expressed concern about the safety of certain devices under review by the agency. They expressed their concern to the President's transition team and to Congress. They

also contacted the Office of Special Counsel, which is an agency, as you know, created by Congress to receive whistleblower complaints and protect whistleblowers from retaliation.

The FDA knew that contacts between whistleblowers and the Office of Special Counsel are confidential and protected by law. However, the FDA was intently spying on whistleblowers. There was no effort to avoid snooping on legally protected communications.

This surveillance was much more intense than routinely monitoring of government employees on government computers. It was far more invasive than what would be necessary to detect inappropriate use of computer systems.

The agency captured a picture of whatever was on the screen every 5 seconds, as you have said, and recorded every keystroke typed. Again, the FDA did not monitor every FDA employee this aggressively, just the whistleblowers.

When we were—first spoke to the FDA in January 2012, they tried to dodge the issue. When I started asking questions, FDA officials seemed to suffer from a sudden case of collective amnesia.

It took the FDA more than 6 months to answer my letter asking about its surveillance of its own employees. When I finally received a response, it didn't even answer the simplest of questions, such as who authorized the targeted operation. Worse than that, it was misleading in its denials about intentionally intercepting communications with Congress.

When I asked them why they couldn't just answer some simple questions, they told my staff that the response was under review by, "the appropriate authorities in the administration." The FDA's non-answers and doublespeak would have fit right into some George Orwell novel.

The work our staffs have done together uncovered answers to many of those initial questions. Today we will hear from some of the FDA employees involved in the surveillance.

There can be legitimate reasons to monitor the use of government computers by government employees; however, as our joint report shows, FDA officials gave little, if any, thought to the legal limits that might restrict their power to monitor their employees.

No one at the FDA made any attempt to limit the collection of legally protected communications with attorneys, with the Office of Special Counsel, or with Congress. The FDA trampled on the privacy of its employees and their right to make legally protected disclosures of waste, fraud, and abuse.

These whistleblowers thought the FDA was caving to pressure from the companies that were applying for FDA approval. I don't know whether they were right. But they have a legal right to express those concerns.

After expressing their safety concerns, two whistleblowers were fired, two more were forced to leave FDA, and five of them were subjected to an intense spying campaign.

At the beginning of FDA Commissioner Hamburg's term, she said that whistleblowers exposed critical issues within the FDA. She vowed to create a culture that values whistleblowers.

By the way, that is a promise I have had from several people predecessor to her coming to my office, wanting confirmation, making those same promises.

In fact, in 2009, Commissioner Hamburg said “I think whistleblowers serve an important role.”

I wanted to believe Commissioner Hamburg when she testified before the Senate during her confirmation. I wanted to believe her when she said she would protect whistleblowers at the FDA. However, in this case, the FDA was certainly not a whistleblower-friendly place to work, and I have spoken about how that’s been the case since at least my involvement since 2003.

The FDA managers believed that the whistleblowers were leaking confidential information improperly, but the managers who—claimed that there were many other problems with the job performance of the targeted employees.

Performance issues, of course, should be handled by directly supervising and managing employees. Instead, the FDA asked the HHS Office of Inspector General to investigate whether the employers had violated the law.

The Inspector General declined on multiple occasions, but FDA managers kept asking for a criminal inquiry. Rather than simply managing its employees, the FDA then started spying on them.

The managers kept looking for information that would convince the Inspector General to seek criminal prosecution. It was sort of management by investigation. And, of course, that’s no way to run an agency.

According to the OIG, and later the Department of Justice, the FDA had no evidence of any criminal wrongdoing by the whistleblowers. None whatsoever was ever found.

The FDA spent months using intrusive realtime surveillance of their employees’ computers looking for evidence of a crime. That time and effort would have been better spent supervising and managing the employees directly and making sure the employees were doing their job and not bothered from doing their job.

The FDA claimed that their employees had no expectation of privacy on their FDA computers. However, when interviewed by congressional investigators, none of the FDA officials were willing to accept full responsibility for authorizing the surveillance. Apparently, no one was properly supervising this invasive surveillance program.

The monitoring software used was so comprehensive it took countless hours just to review all the material. It was a detailed record of everything each of the scientists did all day, every day, for months. Hundreds of thousands of screen images had to be reviewed by FDA contractors, all at taxpayers’ expense.

So what kind of legal guidance was provided to these contractors about what they could capture? None. We would not have known the full extent of the spying today if the FDA had not accidentally released 80,000 pages of fruits of its spying on the Internet.

Talk about adding insult to injury. After collecting all of this information, in an effort to supposedly prevent leaks, the same agency ends up posting all of those documents online for the world to see.

In these internal documents that FDA never wanted the public to see, it referred to the whistleblowers as “collaborators.” So you understand what I mean when I say whistleblowers are about as welcome in an agency as a skunk at a picnic.

FDA referred to our staffers as “ancillary actors.” And they happened to refer to newspaper reporters as “media outlet actors.”

Let me tell you, you wouldn’t be doing any congressional investigation—well, you might do a little bit, because we could obviously ferret out some—but we wouldn’t be doing 90 percent of what we do on protecting whistleblowers and congressional oversight if it wasn’t enterprising newspaper or media people or whistleblowers coming forth with some things that they find wrong that we don’t even know where the skeletons are buried in the bureaucracy of this big government of ours. But, anyway, so they are collaborators, they are ancillary actors, or they are media outlet actors.

The FDA claimed it was a mistake made by the company it hired to convert surveillance records for legal review. And, of course, that wasn’t true. The FDA incorrectly filled out a purchase order for the work. The FDA did not mark the documents as confidential or sensitive. It didn’t even fill out the form until after the work had been done.

Our inquiry uncovered no record that the private contractors were told that the documents were sensitive. So, the FDA failed to classify these documents as sensitive and then tried to blame the small business company that it hired to convert the documents. This is the scene that comes up time and time again in this entire story that you are looking into today.

The FDA has failed to accept responsibility for its actions or impose accountability. This is from an agency that purportedly wants to foster a culture where whistleblowers are valued, based upon Director Hamburg’s testimony to our committee.

The FDA’s actions are, of course, disappointing, not just disappointing because of the history that we are now—of this history, but over a long period of time. And it was supposed to change when this commissioner was appointed.

But it would be even worse if that agency fails to learn from its mistakes. And since 2003, I—and maybe people before me would say the same thing—would say that they have been looking for learning from the mistakes of the past. It doesn’t seem to happen.

And most of these are just simple respect for the scientific process because, if you leave the politics out of it and let scientists do it, the scientific process of one scientist checking on another scientist’s work will prove itself, or that scientist isn’t going to be worth anything.

These policies need to ensure that any monitoring is limited to achieving only the legitimate purpose. Watching on employees every minute leads to a culture of intimidation and fear, which not just the FDA, but bureaucracies generally, want whistleblowers to know about so that they don’t tell what they know is wrong. And, of course, that’s no way to encourage whistleblowers or it’s no way to show that you value their concerns.

I thank you very much.

Chairman ISSA. Thank you.

[Prepared Statement of Senator Grassley follows:]

Statement of Senator Charles E. Grassley
Before the United States House of Representatives
Committee on Oversight and Government Reform
Hearing, "Limitless Surveillance at the FDA: Protecting the Rights of Federal Whistleblowers"
February 26, 2014

Thank you, Chairman Issa, for calling this important hearing and for the great work you and your staff have done.

Together, we have conducted a detailed investigation into the Food and Drug Administration's (FDA) aggressive surveillance of whistleblowers.

A group of FDA scientists expressed concerns about the safety of certain devices under review by the agency.

They expressed their concerns to the President's transition team and to Congress.

They also contacted the Office of Special Counsel, which is an agency created by Congress to receive whistleblower complaints and protect whistleblowers from retaliation.

The FDA knew that contacts between whistleblowers and the Office of Special Counsel are confidential and protected by law.

However, the FDA was intently spying on the whistleblowers.

There was no effort to avoid snooping on legally protected communications.

This surveillance was much more intense than the routine monitoring of government employees on government computers.

It was far more invasive than what would be necessary to detect inappropriate use of the computer systems.

The agency captured a picture of whatever was on the screen every five seconds, and recorded every keystroke typed.

Again, the FDA did not monitor every FDA employee this aggressively -- just the whistleblowers.

When we first spoke to the FDA in January 2012, they tried to dodge the issue.

When I started asking questions, FDA officials seemed to suffer from a sudden case of collective amnesia.

It took the FDA more than six months to answer my letter asking about its surveillance of its own employees.

When I finally received the response, it didn't even answer the simplest of questions, such as who authorized this targeted operation.

Worse than that, it was misleading in its denials about intentionally intercepting communications with Congress.

When I asked them why they couldn't just answer some simple questions, they told my staff that the response was under review by the "appropriate officials in the Administration."

The FDA's non-answers and double-speak would have fit right into a George Orwell novel.

The work our staffs have done together uncovered answers to many of those initial questions.

Today, we will hear from some of the FDA employees involved in the surveillance.

There can be legitimate reasons to monitor the use of government computers by government employees.

However, as our joint report shows, FDA officials gave little, if any, thought to the legal limits that might restrict their power to monitor employees.

No one at the FDA made any attempt to limit the collection of legally protected communications with attorneys, with the Office of Special Counsel, or with Congress.

The FDA trampled on the privacy of its employees and their right to make legally protected disclosures of waste, fraud, or abuse.

These whistleblowers thought the FDA was caving to pressure from the companies that were applying for FDA approval.

I don't know whether they were right, but they have a legal right to express those concerns.

After expressing their safety concerns, two whistleblowers were fired.

Two more were forced to leave the FDA.

And five of them were subjected to an intense spying campaign.

At the beginning of FDA Commissioner Hamburg's term, she said that whistleblowers exposed critical issues within the FDA.

She vowed to create a culture that values whistleblowers.

In fact, in 2009, she said, and I quote, "I think whistleblowers serve an important role."

I wanted to believe Commissioner Hamburg when she testified before the Senate during her confirmation.

I wanted to believe her when she said she would protect whistleblowers at the FDA.

However, in this case, the FDA was certainly not a whistleblower-friendly place to work.

FDA managers believed that the whistleblowers were leaking confidential information improperly.

But the managers also claimed that there were many other problems with the job performance of the targeted employees.

Performance issues should be handled by directly supervising and managing employees.

Instead, the FDA asked the HHS Office of Inspector General to investigate whether the whistleblowers had violated the law.

The Inspector General declined on multiple occasions, but FDA managers kept asking for a criminal inquiry.

Rather than simply managing its employees, the FDA started spying on them.

The managers kept looking for information that would convince the Inspector General to seek a criminal prosecution.

It was a sort of management by investigation.

That's no way to run an agency.

According to the OIG and later the Department of Justice, the FDA had no evidence of any criminal wrongdoing by the whistleblowers.

None would ever be found.

The FDA spent months using intrusive real-time surveillance of their employees' computers, looking for evidence of a crime.

That time and effort would have been better spent supervising and managing the employees directly.

FDA claimed that their employees had no expectation of privacy on their FDA computers.

However, when interviewed by congressional investigators, none of the FDA officials were willing to accept full responsibility for authorizing the surveillance.

Apparently, no one was properly supervising this invasive surveillance program.

The monitoring software used was so comprehensive, it took countless hours just to review all of the material.

It was a detailed record of everything each of the scientists did, all day, every day, for months.

Hundreds of thousands of screen images had to be reviewed by FDA contractors, all at taxpayer expense.

So what kind of legal guidance was provided to these contractors about what they could capture?

None.

We would not have known the full extent of the spying today if the FDA had not accidentally released 80,000 pages of the fruits of its spying on the Internet.

Talk about adding insult to injury.

After collecting all of this information in an effort to supposedly prevent leaks, the same agency ends up posting all those documents online for the world to see.

In these internal documents that FDA never wanted the public to see, it refers to the whistleblowers as "collaborators."

FDA refers to congressional staff as "ancillary actors."

FDA refers to the newspaper reporters as "media outlet actors."

The FDA claimed it was a mistake made by the company it hired to convert surveillance records for legal review.

That wasn't true.

The FDA incorrectly filled out a purchase order for the work.

The FDA did not mark the documents as confidential or sensitive, and it didn't even fill out the form until after the work had been done.

Our inquiry uncovered no record that the private contractor was told that the documents were sensitive.

So, the FDA failed to classify these documents as sensitive and then tried to blame the small business it hired to convert the documents.

This is the theme that comes up time and again in this story.

The FDA has failed to accept responsibility for its actions or impose accountability.

This is from an agency that purportedly wants to foster a culture where whistleblowers are valued.

The FDA's actions are disappointing.

But, it would be even worse if it fails to learn from its mistakes.

All agencies need to learn from these mistakes.

There need to be more comprehensive, policies on employee computer monitoring across the entire government.

These policies need to ensure that any monitoring is limited to achieve only a legitimate purpose.

Watching an employee's every move leads to a culture of intimidation and fear.

That's no way to encourage whistleblowers or value their concerns.

Thank you for inviting me to testify today.

Chairman ISSA. And if you would take a few questions from the ranking member, I would appreciate it.

Senator GRASSLEY. Yes.

Chairman ISSA. Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Senator Grassley. And I really do thank you for being here today. Thank you for your patience.

I have the utmost respect for you and your legacy as a champion of whistleblowers and whistleblower protections, and I really—on behalf of the American people, I thank you.

Senator GRASSLEY. Thank you.

Mr. CUMMINGS. As I said earlier, this has not traditionally been a partisan topic, I don't think. You and Senator Akaka both sponsored the Whistleblower Protection Enhancement Act, and Chairman Issa and I sponsored the House version of that bill. I assume you agree that we accomplish much more when we are working together.

Would you agree with that?

Senator GRASSLEY. I have found—

Mr. CUMMINGS. I heard what you said about the skunk and all that.

Senator GRASSLEY. Well, listen. I think your question is trying to put me between you two people, and I don't relish being there.

But I have found in the United States Senate—I don't want to talk about the House of Representatives—I have found in the United States Senate that not a whole lot gets done if it's not done in a bipartisan way.

But that's because our two institutions are different. We function under a 60-vote rule that requires, when you have 55 of one party, 45 of the other, you have got to do something in a bipartisan way.

And I have also found, as a member of the minority, that it makes a real difference who is chairman of the committee. When I was working with Senator Baucus on the Finance Committee and he was in the majority, I didn't get much response from any administration without the help of the chairman.

Mr. CUMMINGS. Have you had an opportunity to talk to the whistleblowers?

Senator GRASSLEY. We have only talked to their attorneys.

Mr. CUMMINGS. I see.

Chairman Issa and I had a good discussion this morning prior to the hearing. And one of the things that he raised—and I agreed—it seems like this—and I want the witnesses to hear this—it seems to me that the issue comes down to this: When—first of all, there was a situation which screamed out for somebody to look into it. In other words, New York Times writing articles with trade secrets, it seems like the agency had a duty to at least look into it.

Would you agree with that?

Senator GRASSLEY. Would you please ask your question again.

Mr. CUMMINGS. In other words, the way this whole thing started, apparently, are some stories in the New York Times with trade secrets in the New York Times that weren't supposed to be there.

Senator GRASSLEY. Okay.

Mr. CUMMINGS. And so I think it started off legitimately saying, “Okay. We have got a problem here because this information is not supposed to be in the New York Times.”

So would you agree that, at least starting, they had something that they needed to look into? Now, I am not saying they did it right. I am just asking you—

Senator GRASSLEY. Okay. I am not sure that I can answer your question.

Mr. CUMMINGS. Okay.

Senator GRASSLEY. But let me see if I can speak to it and give you some satisfaction.

I think it gets down to a point of whether or not the information was accurate or not that these whistleblowers were talking about. We have not looked into the accuracy of that information. We have only looked into it from the standpoint that some people say there is some problems.

And that’s where you get back to the point that I have made a couple times, not about the skunk, but about the scientific process, that we want an environment within the FDA where the scientific process works its way out and is not interfered by people that aren’t scientists or involved in that process.

And I will only go back to one other instance a long time ago. But we have found that—in one instance years ago, we found email from industry that said, “Well, if you have got a problem with our product, talk to us.”

Well, the point is that the FDA should not consider a manufacturer or a company across the table from them. The only people that should be across the table from the FDA scientists or regulators are the John Q. Public.

Mr. CUMMINGS. Okay. And so, in this case, a group of FDA employees alleged that certain medical devices may have safety problems.

Now, if their allegations are correct, that is obviously a huge problem for everyone who relies on these types of medical devices when they become ill or get in an accident.

On the other hand, if these allegations are not correct, these FDA employees could be doing damage. They could be keeping safe medical devices off the market and out of the hands of doctors who use them to help people.

And I think that you would agree that we—if devices should be on the market to save people’s lives and make them better, they ought to be there. Would you agree with that?

Senator GRASSLEY. Well, the answer to that is “yes.” But how do you—how is that decision made? It’s not going to be made by us in Congress.

Mr. CUMMINGS. I got that.

Senator GRASSLEY. It’s going to be made by the scientific approach in the FDA.

Mr. CUMMINGS. Just one more question, Mr. Chairman.

Let me just get to this—the key question that the chairman and I were discussing this morning.

It seems to me that, if they had done this—the investigative folk had done this in a retrospective way as opposed to a prospective

way, we probably would not have the issues—as many issues as we have today. Do you think?

Senator GRASSLEY. Well, yes. But I have to surmise—because I can't answer your question. But I have to surmise the reason it worked out the way it worked out is people weren't getting the proper respect within the agency for their opinion.

Mr. CUMMINGS. I see.

Senator GRASSLEY. And their opinion could be wrong. But the scientific process is going to prove whether or not they were right or wrong.

Mr. CUMMINGS. Well, again, I want to thank you for being here. I really appreciate it.

Senator GRASSLEY. Thank you.

Mr. CUMMINGS. And I look forward to working with you.

Senator GRASSLEY. Please do.

Mr. CUMMINGS. We need to get together and meet sometime.

Senator GRASSLEY. I will take you to eat in the Members' dining room, and I will pay for it, if you want to take me up on that.

Mr. CUMMINGS. All righty. Thank you.

Chairman ISSA. Senator Grassley, we know how hard it was for you to say that.

Senator GRASSLEY. And it hurt. But since I said it, I will have to do it.

Mr. CUMMINGS. I will hold you to it, too.

Chairman ISSA. Thank you. We are going to take just a quick recess to set up the table. Thank you, Senator.

[Recess.]

Chairman ISSA. We now welcome our second panel.

Dr. Jeffrey Shuren is the Director of the Center for Devices and Radiological Health at the FDA. Ms. Ruth McKee is the Associate Director for Management and the Executive Officer of the Center for Devices and Radiological Health. Mr. Walter Harris is Chief Operating Officer and Acting Chief Information Officer for the FDA and, presumably, the person that would approve such an activity in the future under the rules. And Ms. Angela Canterbury is the Director of Public Policy for the Project on Government Oversight, or POGO.

And we welcome all of you.

Pursuant to the committee's rules for any non-Senators or House Members, would you please rise and take the oath. And please raise your right hands.

Do you solemnly swear or affirm the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for questions, I would ask that you be as close to 5 minutes as possible in your opening statements. Your entire written opening statement will be placed in the record.

And, Dr. Shuren, I understand you do not have an opening statement. Is that correct?

Dr. SHUREN. That is correct.

Chairman ISSA. Okay. In that case, we go to Ms. McKee.

Ms. MCKEE. I don't have one either. Mr. Harris is speaking.

Chairman ISSA. Okay.
Mr. Harris?

STATEMENT OF WALTER HARRIS

Mr. HARRIS. Good morning, Chairman.

Chairman Issa, Ranking Member Cummings, and members of the committee, I am Walter Harris, the Deputy Commissioner of Operations, Chief Operating Officer, and Acting Chief Information Officer at FDA.

With me is Dr. Jeff Shuren, the Director of FDA's Center for Devices and Radiological Health, and Ruth McKee, CDRH Associate Director for Management.

I am pleased to be here today to discuss issues related to the monitoring of FDA's personnel's use of the agency's IT systems. Safeguarding the confidential information that regulated entities share with FDA is critical to our ability to carry out FDA's public health mission.

FDA routinely receives and reviews trade secrets and confidential commercial information from medical product sponsors. This information is central to FDA's determination of a medical product's safety and efficacy. Without the ability to fully access and secure this proprietary information, FDA cannot accomplish its public health mission.

FDA employees secure the controls throughout our IT enterprise, including the monitoring of FDA personnel's use of government-owned equipment. This and other IT controls supports protections of intellectual property entrusted to FDA from theft or sabotage.

Unauthorized disclosures of information not only violates Federal law and regulations and undermines the integrity of FDA programs, they also can result in civil suits against FDA.

So it's critically important that FDA protects against unauthorized disclosure of such information by agency personnel and for the FDA to appropriately investigate any suspected incidents of unauthorized disclosure.

FDA personnel are regularly advised that they have no reasonable expectation of privacy when using FDA computer networks and that any use of agency IT resources, including email, may be monitored. This notice is provided by a variety of means, including a warning banner that an employee must acknowledge every time he or she logs on to the FDA network, which clearly states that, by logging onto the system, the user consents to having no reasonable expectation of privacy regarding any communications or data in transit or stored on that system.

All FDA users are also made aware of HHS policy that any use of HHS email may not be secure, it is not private, it is not anonymous, it may be subject to disclosure, and that employees do not have the right to, nor expectation, of privacy at any time while using HHS IT resources.

Although FDA has clear legal responsibility and authority to monitor personnel use of agency IT resources, we must carry out such monitoring in a way that recognizes employees' interests and legal protections.

In 2010, FDA suspected that five CDRH employees were using FDA IT systems to send trade secrets or confidential commercial

information outside of FDA, in possible violation of FDA regulations and criminal laws.

To investigate the suspected leaks, FDA employed computer-monitoring software on those employees' government-issued FDA computers, the computer surveillance that is currently the subject of ongoing litigation.

In 2012, the HHS Office of Inspector General, or OIG, was asked to assess whether that monitoring was appropriate and to provide recommendations on how FDA should investigate allegations of improper dissemination of confidential information.

Yesterday the OIG issued its report. Significantly, the OIG found that the CDRH had reasonable concerns that confidential information had been disclosed by the monitored employees without authorization.

The OIG also found that FDA had provided notice through the network log-in banner to those employees that the use of their FDA computers would be monitored.

The OIG found no evidence that FDA obtained or used passwords of any employees' private email accounts, and the OIG found that there were no evidence suggesting that FDA monitoring was designed to capture communications with any particular person, group, including Congress.

Yet, we understand that we must have adequate procedures in place when conducting such monitoring. Indeed, since 2012, we have been reviewing and evaluating our policies for monitoring the use of government-owned computers to ensure they are consistent with the law and with Congress's intent to provide a secure channel for protected disclosures.

In September 2012, Commissioner Hamburg directed FDA leadership to adopt policies for requests to monitor FDA computers to make sure that any monitoring is justified, narrowly tailored and duly authorized, that data derived from monitoring is appropriately stored and controlled, and that monitoring is used for appropriate purposes and takes place for no longer than necessary.

Last September, we issued our interim computer-monitoring policy. This policy provides standards when employee computer monitoring takes place.

It established a special committee to review monitoring requests. It requires that monitoring requests be narrowly tailored in time, scope, and degree. It requires that all requests identify the least invasive approach.

It also requires considerations of alternative methods to address the potential risk, provide documentation standards, and states that no computer monitoring may target communications with law enforcement, the Office of Special Counsel, members of Congress, union officials, or private attorneys.

Notably, yesterday's OIG report acknowledges that our September 2013 interim computer-monitoring policy addresses all of the OIG's recommendations.

In order for FDA to effectively carry out its public health mission, we must be vigilant to protect against the misuse or unauthorized disclosure of confidential information that is regularly entrusted to the agency.

We believe that the policies and procedures we have in place appropriately and effectively balance the individual interests of employees with FDA's critical needs to safeguard the security and integrity of data and IT systems that the agency is entrusted to manage.

Thank you for your commitment to FDA's mission and for the opportunity to testify today about the monitoring of FDA employees' use of agency IT resources and FDA's responsibilities to secure medical product sponsors' confidential information.

I am pleased to answer any questions.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Harris follows:]



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Public Health Service

Food and Drug Administration
Silver Spring, MD 20993

**STATEMENT
OF
WALTER S. HARRIS
DEPUTY COMMISSIONER FOR OPERATIONS AND CHIEF OPERATING OFFICER
FOOD AND DRUG ADMINISTRATION
DEPARTMENT OF HEALTH AND HUMAN SERVICES
BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
MONITORING FDA PERSONNEL'S USE OF AGENCY INFORMATION
TECHNOLOGY SYSTEMS**

February 26, 2014

Release Only On Delivery

INTRODUCTION

Chairman Issa, Ranking Member Cummings, and Members of the Committee, I am Walter S. Harris, Deputy Commissioner for Operations and Chief Operating Officer (COO), and Acting Chief Information Officer (CIO) of the Food and Drug Administration (FDA or the Agency), which is part of the Department of Health and Human Services (HHS). I am pleased to be here today to discuss issues related to the monitoring of FDA personnel's use of Agency information technology (IT) systems.

As FDA's COO, my role is to provide executive direction, leadership, coordination, and guidance for the overall day-to-day administrative operations of FDA, in order to ensure the timely and effective implementation and high-quality delivery of services across the Agency. I am also currently serving as FDA's Acting CIO. As such, I am responsible for establishing and implementing the Agency's incident response plan for responding to the detection of computer security incidents involving FDA information systems and ensuring that appropriate action is taken to minimize the consequences of such incidents. I coordinate with FDA's Office of Chief Counsel (OCC), Office of Criminal Investigations (OCI), and Office of Security Operations (OSO), and with other law enforcement authorities, on actions and activities involving computer monitoring of use of FDA's IT resources and the retrieval of electronic records, where appropriate.

FDA's IT Security (IS) Program, headed by the Agency's Chief Information Security Officer (CISO), directs and implements the IT security program to ensure that adequate and appropriate controls are applied to FDA systems for the protection of privacy, and to ensure confidentiality, integrity, and availability of information. The CISO employs security policies and standards for FDA information systems enterprise-wide in accordance with FDA, HHS, Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST) and other Federal security requirements. Key activities of FDA's IS Services staff include: cyber security and insider-threat detection; IT security operations; security authorization and audit management; policy, awareness, and training; Information Systems Security Officer (ISSO) support; and contingency planning.

Cyber threats, vulnerabilities, and risks to FDA's IT infrastructure of over 18,000 end users, 83 production systems, and 379 applications are on the rise. These threats, vulnerabilities, and risks to the FDA IT infrastructure include, but are not limited to: external threats (i.e., transnational criminal organizations, hackers) and end users leveraging computer access to advance inappropriate activities;¹ the exploitation of sensitive information, which could negatively impact FDA's mission and U.S. national and economic security; and direct threats to FDA critical assets (including the Agency's personnel, processes, programs, and computer systems).

As described further in this testimony, FDA personnel are permitted access to information provided to the Agency by medical product sponsors and others and are required to maintain the

¹ Other insider-related threats include new, sophisticated phishing techniques such as "Vishing," "Tabnabbing," and "Evil Twinning."

strict confidentiality of that information. However, security breaches involving FDA personnel have occurred in the past.

For example, in March 2012, Cheng Yi Liang, a former FDA chemist, was sentenced to 60 months in prison² for engaging in insider trading on multiple occasions based on material, non-public information he obtained in his capacity as an FDA scientist.³ Liang had been employed as a chemist for more than 15 years by FDA's Office of New Drug Quality Assessment (NDQA), and through his work at NDQA, had access to FDA's password-protected internal tracking system for new drug applications. Much of the information accessible on that computer tracking system, "Document Archiving, Reporting, and Regulatory Tracking System," known as DARRTS, constitutes proprietary, non-public information regarding pharmaceutical companies that submit their experimental drugs for FDA review.

In his plea, Liang admitted that between 2006 and 2011, using non-public information from DARRTS and other sources, he traded in the securities of pharmaceutical companies in violation of the duties of trust and confidence that he owed FDA as an employee. As stated in FDA's post-conviction Proposal to Debar Liang:

² Liang's sentence was announced by the U.S. Department of Justice, the U.S. Attorney for the District of Maryland, the Federal Bureau of Investigation, and the HHS Office of the Inspector General (OIG). See U.S. Department of Justice, "Former FDA Chemist Sentenced to 60 Months in Prison for Insider Trading" (March 5, 2012), available at <http://www.fbi.gov/washingtondc/press-releases/2012/former-fda-chemist-sentenced-to-60-months-in-prison-for-insider-trading>. "Mr. Liang violated his duty of loyalty to the FDA and profited from inside information," said U.S. Attorney for the District of Maryland Rod J. Rosenstein. "Liang brazenly sought to profit based on sensitive, insider information. What he didn't know is that investigators have been utilizing sophisticated technical tools to identify and track criminal behavior. We will continue to insist that Federal Government employee conduct be held to the highest of standards," said Elton Malone, Special Agent in Charge, HHS, OIG Office of Investigations, Special Investigations Branch. "Mr. Liang breached the trust of his employment by obtaining sensitive information and using it for his own profit," said James W. McJunkin, former Assistant Director in Charge of FBI's Washington Field Office.

³ Liang was also ordered to forfeit \$3.7 million, representing the proceeds of the insider-trading scheme.

“As an FDA employee who worked in CDER’s Office of New Drug Quality Assessment, you had access to the DARRTS database containing non-public information about the status of approvals for new drugs. FDA is required by statute and its regulations to keep certain information relating to drug approvals confidential. You exploited the position with which you were entrusted as a scientist at FDA to access confidential information in the DARRTS database..., and you used that information in a scheme for personal gain. You accessed confidential information... repeatedly as part of your scheme, and set up brokerage accounts in the names of others in furtherance of that scheme. * * *

The Standards of Ethical Conduct for Employees of the Executive Branch require that all employees shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure. You were aware of your responsibility to comply with this requirement, and you violated that responsibility.”⁴

In addition to the criminal conviction, Liang was ultimately debarred from providing services in any capacity to a person that has an approved or pending drug product application,⁵ based on a finding that he had been convicted of a felony under Federal law for conduct relating to the development or approval of a drug product.

Public service is a public trust. Each and every employee of FDA and HHS has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws, and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, all executive branch employees are required to respect and adhere to principles of ethical conduct set forth by applicable Federal law and regulations.⁶

⁴ See FDA, “Proposal to Debar, Notice of Opportunity for Hearing,” Docket No. FDA-2012-N-0783 (Nov. 6, 2012), available at <http://www.fda.gov/regulatoryinformation/foi/electronicreadingroom/ucm334415.htm>.

⁵ See FDA, “Cheng Yi Liang: Debarment Order,” 78 *Fed. Reg.* 14556, Docket No. FDA-2012-N-0783 (March 6, 2013), available at <http://www.gpo.gov/fdsys/pkg/FR-2013-03-06/html/2013-05160.htm>.

⁶ See U.S. Office of Government Ethics, “Standards of Ethical Conduct for Employees of the Executive Branch” (June 2009), available at

As FDA employees work to advance the health and welfare of the public, we seek to maintain the highest standards of ethical conduct: the essence of good government is the personal responsibility that each public servant feels for the public trust that he/she holds. FDA employees are expected to be people of integrity and to observe the highest standards of conduct. Because of FDA's special regulatory responsibilities, its personnel must carry on the Agency's business effectively, objectively, and without even the appearance of impropriety, and Agency personnel may not use, or permit others to use, official information not available to the general public for gain or to advance a private interest.⁷

The scope, breadth, and extent of risks faced by FDA in the event of information security breaches are significant and require the utmost vigilance on the part of the Agency and all of its personnel to ensure that the valuable data entrusted to FDA is protected from both internal and external threats and vulnerabilities. As described in this testimony, safeguarding the confidential information that regulated entities share with FDA is critical to the Agency's ability to carry out its public health mission, and FDA has adopted policies and procedures to preserve the data security of its confidential information.

<http://www.oge.gov/displaytemplates/statutesregulationsdetail.aspx?id=293&langtype=1033>, and the statutes and regulations cited therein.

⁷ See, e.g., FDA, "Investigations Operations Manual," Subchapter 1.6, "Public Relations, Ethics and Conduct," available at *<http://www.fda.gov/ICEC/Inspections/IOM/ucm122505.htm>*.

FDA's Responsibility to Protect Confidential Information

FDA protects and promotes the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; by ensuring the safety and security of our nation's food supply, cosmetics, and products that emit radiation; and by regulating tobacco products. The Agency also helps to advance the public health by helping to speed innovations and by helping the public get the accurate, science-based information that it needs to properly use medicines and medical devices in a way to maintain and improve their health.

FDA's ability to fulfill the Agency's public health mission is closely tied to our ability to protect and safeguard confidential information that is submitted by regulated entities and others, and is entrusted to FDA. The Agency routinely receives and reviews trade secrets and confidential commercial information. For example, medical product sponsors, including manufacturers, are expected to provide FDA with detailed and complete information about how a product works, how it is made, and what materials or ingredients are used to make it. This information is central to the Agency's full and adequate evaluation of the data and determination of a medical product's safety and efficacy. Without the ability to fully access—and to secure—this proprietary information, the Agency cannot accomplish its public health mission.

In many instances, the mere fact that a firm has made a submission to FDA 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 advantage by providing otherwise unavailable insights into the development process, and disclosure of such details could undermine incentives for innovation and competition in the commercial market. FDA's ability to carry out its responsibilities effectively depends on its ability to have timely access to this highly sensitive information, and improper disclosure could hamper FDA's ability to obtain such information.

The E-Government Act of 2002⁸ recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled 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 its operations and assets, including those provided or managed by another agency, contractor, or other source.

HHS has developed policies to comply with FISMA, including the HHS Office of the Chief Information Officer's (OCIO) "HHS-OCIO Policy for Information Systems Security and Privacy" (the HHS-OCIO Policy for ISSP),⁹ which provides direction to the IT security programs of the Department's Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs) for the security and privacy of HHS data.

⁸ Pub. L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), available at <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.

⁹ HHS, "HHS-OCIO Policy for Information Systems Security and Privacy," HHS-OCIO-2011-0003 (rev. July 7, 2011), available at <http://www.hhs.gov/ocio/policy/hhs-ocio-2011-0003.html>. The HHS-OCIO Policy establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of HHS OPDIVs and STAFFDIVs, including FDA.

FDA employees are subject to monitoring of their use of government-owned equipment in accordance with policies developed to comply with FISMA.¹⁰

As required under FISMA, FDA employs IT security controls throughout the Agency's IT Enterprise. These IT controls are employed to ensure the confidentiality, integrity, and availability of FDA data and are consistent with the management, operational, and technical controls outlined in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," as amended.¹¹ These IT controls broadly include logging of all system events, monitoring of data entering and leaving the FDA IT Enterprise, and ensuring authorized access to systems. The security controls are further employed to support the protection of intellectual property entrusted to FDA from theft or sabotage.

In addition to FISMA, there are other laws that expressly prohibit FDA personnel from disclosing trade secrets and confidential commercial information unless authorized by law. For example, section 1905 of title 18 of the Federal criminal code states:

"Whoever, being an officer or employee of the United States or of any department or agency thereof, . . . publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as

¹⁰ In addition, FDA may monitor FDA e-mail accounts and other IT resources, when appropriate, such as in support of authorized personnel investigations or law enforcement activities.

¹¹ Available at <http://csrc.nist.gov/publications/PubsSPs.html>.

provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.”¹²

The Federal Food, Drug, and Cosmetic Act (FD&C Act) also includes provisions specifically prohibiting Federal employees from disclosing proprietary information. For example, section 301(j) (“Prohibited Acts”) of the FD&C Act expressly prohibits “[t]he using by any person to his own advantage, or revealing, other than to the Secretary or officers or employees of the Department, or to the courts when relevant in any judicial proceeding under this Act, any information acquired under authority of section 404, 409, 412, 414, 505, 510, 512, 513, 514, 515, 516, 518, 519, 520, 571, 572, 573, 704, 708, 721, 904, 905, 906, 907, 908, 909, or 920(b) concerning any method or process which as a trade secret is entitled to protection...”¹³

FDA has promulgated numerous regulations implementing the protections provided by the FD&C Act and other statutes for confidential information. For example, FDA’s principal regulation regarding non-disclosure of trade secrets and confidential commercial information states that “[d]ata and information submitted or divulged to [FDA] which fall within the definitions of a trade secret or confidential commercial or financial information are not available for public disclosure.”¹⁴ The Agency also has several product-specific regulations. For example, under 21 CFR 314.430, 601.51, and 814.9, FDA is prohibited, with limited exceptions, from disclosing the existence of a marketing application for a drug or biological product, or a premarket approval application for a device, unless the existence of the application has been previously publicly disclosed or acknowledged by the sponsor. There are similar restrictions

¹² 18 U.S.C. § 1905, “Disclosure of Confidential Information Generally,” available at <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/pdf/USCODE-2012-title18-part1-chap93-sec1905.pdf>.
¹³ 21 U.S.C. 331(j), available at <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title21/pdf/USCODE-2012-title21-chap9-subchap11-sec331.pdf>.

regarding disclosing the existence of a premarket notification submission (“510(k)”) for a device,¹⁵ and the same regulations generally prohibit FDA from releasing any information from or about a pending application or 510(k).

Unauthorized disclosures of information not only violate Federal laws and regulations and undermine the integrity of FDA programs, they also can result in civil suits against FDA. Accordingly, it is critically important that FDA protect against unauthorized disclosure of such information, including by Agency personnel, and for FDA to appropriately investigate suspected incidents of unauthorized disclosure of such information.

FDA Staff Awareness of Privacy Limitations and IT System Monitoring¹⁶

Because, as described above, FDA personnel are subject to monitoring of their use of Agency IT systems, resources, and equipment, Agency personnel are regularly advised that they have no reasonable expectation of privacy when making use of the FDA computer network, and that any use of Agency IT resources, including e-mail, may be monitored. Such notice is provided to FDA personnel by variety of means.

LOG-IN BANNER: Since September 2010, all users of the FDA computer network have received notice upon logging into an FDA computer that they should have no reasonable

¹⁴ 21 CFR 20.61, available at <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=20.61>.

¹⁵ 21 CFR 807.95, available at <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=807.95>.

¹⁶ There is an active Federal litigation, styled *Hardy, et al. v. Hamburg, et al.*, Civ. No. 1:11-cv-01739-RBW (D.D.C. filed Sept. 28, 2011), that involves some of the issues discussed here. The litigation’s constraints with respect to the rights of individuals and governmental legal prerogatives will limit the Agency’s responses to questions related to matters involved in the litigation.

expectation of privacy when utilizing the FDA computer system. Upon logging on to the FDA network, users immediately receive the following warning message:

- - - - WARNING - - WARNING - - WARNING - - WARNING - - WARNING - - - -

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 system, 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.

Prior to August 30, 2010, a similar, but not identical, banner was used.¹⁷

FDA's deployment of the warning banner is in accordance with applicable HHS policy, which requires the use of a warning banner on all Department IT systems.¹⁸ The warning banner must

¹⁷ The prior log-in banner read as follows: "This is a Food and Drug Administration (FDA) computer system and is provided for the processing of official U.S. Government information only. All data contained on this computer system is owned by the FDA and may, for the purpose of protecting the rights and property of the FDA, be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed by and to authorized personnel. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISCLOSURE. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Authorized personnel may give to law enforcement officials any potential evidence of crime found on FDA computer systems. Unauthorized access or use of this computer system and software may subject violators to criminal, civil, and/or administrative action. The standards for ethical conduct for employees of the Executive Branch (5 CFR 2635.704) do not permit the use of government property, including computers, for other than authorized purposes."

¹⁸ For example, Section 4.1.3 of the HHS-OCIO Policy for ISSP requires HHS OPDIVs and STAFFDIVs to ensure that information systems provide adequate, risk-based protection in certain control areas by using the appropriate baseline security controls as established in NIST Special Publication 800-53, Rev. 3, "Recommended Security Controls for Federal Information Systems" (August 2009). Control AC-8 of NIST SP 800-53 states: "The information system: (a) Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government

state that, by accessing an HHS IT system (e.g., logging onto a Department computer or network), the user consents to having no reasonable expectation of privacy regarding any communication or data transiting or stored on that system, and the user understands that, at any time, the Department may monitor the use of HHS IT resources.

ANNUAL FDA SECURITY AWARENESS TRAINING: All FDA users are required to complete Computer Security Awareness Training (CSAT) annually, and new hires are required to complete security awareness training within two weeks of their hire date. Computer accounts are disabled for any individuals who do not complete the annual training, and access is not restored until completion of the CSAT for the previous year is confirmed. Current topics of the Security Awareness Training include: security risk awareness and threat sources, protecting sensitive information, portable devices, Internet threats, access control, remote access, reporting incidents, and user responsibilities. The Security Awareness Training also includes the reminder that all network activities may be monitored. All users must also acknowledge the HHS Rules of Behavior¹⁹ to receive the certificate of completion for the FDA Security Awareness Training. Among other things, the acknowledgement of the HHS Rules of Behavior reminds the user that they have no expectation of privacy while accessing HHS computers, networks, or e-mail and that they must not “conduct official government business or transmit/store sensitive HHS information using non-authorized equipment or services.”

information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.” See http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

¹⁹ HHS, Office of the CIO, “Rules of Behavior for Use of HHS Information Resources,” Doc. No. HHS-OCIO-2013-0003S (Sept. 24, 2013), available at <http://www.hhs.gov/ocio/policy/hhs-rob.html>. Prior to 2013, there existed

HHS POLICY ON PERSONAL USE OF AGENCY IT RESOURCES: All FDA personnel are subject to the HHS Information Resources Management (IRM) “Policy for Personal Use of Information Technology Resources,” which states:

“5.7 Any use of HHS IT resources, including e-mail, is made with the understanding that such use may not be secure, is not private, is not anonymous and may be subject to disclosure under the Freedom of Information Act (FOIA). HHS employees do not have a right to, nor shall they have an expectation of, privacy while using HHS IT resources at any time, including accessing the Internet through HHS gateways and using e-mail, which may be subject to release pursuant to the Freedom of Information Act. To the extent that employees wish that their private activities remain private, they shall avoid making personal use of HHS IT resources.

5.8 Electronic data communications may be disclosed within the Department to employees who have a need to know in the performance of their duties (such as, with manager approval technical staff may employ monitoring tools in order to maximize the utilization of their resources, which may include the detection of inappropriate use).”²⁰

HHS RULES OF BEHAVIOR FOR USE OF INFORMATION RESOURCES: The Department’s “Rules of Behavior for Use of HHS Information Resources”²¹ (Rules of Behavior), which is issued under the authority of the HHS-OCIO Policy for ISSP, provides the rules that govern the appropriate use of all HHS information resources for Department users, including Federal employees, contractors, and other systems users. The Rules of Behavior require HHS personnel

a 2010, and 2008, version of the HHS Rules of Behavior; each of those versions included a similar certification regarding HHS personnel’s consent to having no expectation of privacy while accessing HHS IT systems.

²⁰ “HHS IRM Policy for Personal Use of Information Technology Resources,” HHS-OCIO-2006-0001 (Feb. 17, 2006), available at <http://www.hhs.gov/ocio/policy/2006-0001.html>.

²¹ HHS, Office of the CIO, “Rules of Behavior for Use of HHS Information Resources,” Doc. No. HHS-OCIO-2013-0003S (Sept. 24, 2013), available at <http://www.hhs.gov/ocio/policy/hhs-rob.html>. All new users of HHS information resources must read the HHS Rules of Behavior and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. By signing the form, users reaffirm their knowledge of, and agreement to adhere to, the HHS Rules of Behavior.

to certify, among other things, that they “[u]nderstand and consent to having no expectation of privacy while accessing HHS computers, networks, or e-mail.”²²

As detailed above, FDA advises all of its personnel on a regular and frequent basis that, as required by Federal law and in accordance with well-established Department and Agency policies, FDA personnel have no reasonable expectation of privacy when using FDA’s IT resources, and that any use of such resources, including e-mail, may be monitored.

FDA’s Policies to Appropriately Balance Employee Interests and Data Security

Although, as described above, FDA has clear legal responsibility and authority to monitor personnel use of the Agency’s IT resources, FDA also has a responsibility to carry out any such computer monitoring in a manner that recognizes employee interests and relevant legal protections. Therefore, HHS and FDA have put in place a number of policies and procedures to appropriately balance the interests of individual employees and the Agency’s need to preserve the integrity of its IT resources and the security of confidential information.

For example, FDA has put in place appropriate oversight and controls to ensure that any monitoring is justified, reasonable in scope, and duly authorized; that data derived as a result of monitoring is appropriately stored and controlled; and that monitoring is utilized for appropriate purposes and takes place for no longer than necessary. The Agency complies with all applicable Federal laws that protect employee interests, including (but not limited to) the

²² HHS Rules of Behavior at p. 3.

Privacy Act of 1974, the privacy and FISMA provisions of the E-Government Act of 2002,²³ the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (NO FEAR Act),²⁴ and the Whistleblower Protection Enhancement Act of 2012²⁵ (the Whistleblower Protection Act or WPA), as well as all administration policy directives issued in furtherance of those Acts.

Under the NO FEAR Act,²⁶ employees are required to undergo training every two years on their rights and protections under the antidiscrimination and whistleblower laws. FDA offers an online training course on the NO FEAR Act to all new hires and current employees.

In addition, FDA leadership has reminded Agency staff regarding the legal protections under the WPA. In February 2009, then-acting FDA Commissioner Dr. Frank Torti issued an Agency-wide memorandum detailing whistleblower protections for FDA employees. Again, in January 2010, FDA Commissioner Dr. Margaret Hamburg issued an “all-hands” memo to all FDA employees affirming the Agency’s strong support for the Whistleblower Protection Act of 1989, which affords employees the legal protection to make a protected disclosure without fear of reprisal. In that memo, Dr. Hamburg reminded employees of the U.S. Office of Special Counsel’s (OSC) process for addressing complaints of whistleblower retaliation, stating that “[r]eprisal against individuals will not be tolerated for disclosure of information in which the employee believes there is reasonable evidence of violation of any law, rule or regulation ... or a

²³ Pub. L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), available at <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.

²⁴ Pub. L. 107-174, codified at 5 U.S.C. § 2301 note (2011).

²⁵ Whistleblower Protection Act of 1989 (Pub. L. 101-12), codified at 5 U.S.C. § 2302 (2011).

²⁶ Pub. L. 107-174, codified at 5 U.S.C. § 2301 note (2011).

substantial and specific danger to public health or safety.” Dr. Hamburg further directed employees to an online training course and provided OSC’s web address and phone number.

In June 2012, Federal agencies, including FDA, received two memoranda from OMB and OSC relating to legal restrictions and guidelines for the monitoring of employee communications, including electronic mail.²⁷ Since then, FDA has continued to review and evaluate the Agency’s policies and practices for monitoring the use of government-owned computers issued to FDA personnel to ensure that they are consistent with the law and with Congress’ intent to provide a secure channel for protected disclosures.

In August 2012, Dr. Hamburg directed FDA’s Office of Information Management not to deploy, without written approval by the Agency’s Chief Counsel or her delegate, certain software that enables the prospective collection of data on the use of the specific computer onto which it is installed.

In September 2012, Dr. Hamburg directed FDA’s CIO to put into place procedures to strengthen the Agency’s ability to effectively analyze, authorize, and document requests for monitoring of Agency personnel’s FDA computers to ensure that any such monitoring would continue to be conducted in an appropriate manner. FDA’s CIO and Chief Counsel were directed to develop a written policy for contemporaneous monitoring of individual FDA computers that would require express written authorization of such monitoring by the Commissioner, a Deputy Commissioner, or the COO, with documentation of the reason for the monitoring. The policy would authorize

²⁷ OMB, “Memorandum for Chief Information Officers and General Counsels” (June 20, 2012); OSC, “Memorandum for Executive Departments and Agencies” (June 20, 2012).

computer monitoring only pursuant to a request from outside law enforcement or the HHS Inspector General, or in the event that there were reasonable grounds to believe that the individual being monitored was responsible for unauthorized disclosure of legally protected information or had violated Department or Agency personnel, administrative, or IT policy. Any authorized monitoring would be required to be as narrow, time-limited, and non-invasive as appropriate to accomplish the stated information-gathering objective. Legal review would be required to determine whether the monitoring is legally supportable, including consideration of whether the proposed monitoring is consistent with all applicable legal requirements, including the WPA. The CIO would be required to review any authorized computer monitoring on a monthly basis to assess whether it remains justified or must be discontinued, and if continued, that decision would be required to be explained in writing.

In June 2013, the HHS Assistant Secretary for Administration directed each HHS OPDIV and STAFFDIV Head, working with their respective OPDIV CIO, to establish policies and procedures to strengthen the ability to effectively document, analyze, authorize, and manage requests for monitoring personnel use of HHS IT resources.²⁸ In addition to the elements described above, the June 2013 directive specifically stated that no monitoring may target communications with law enforcement entities, the OSC, members of Congress or their staff, employee union officials, or private attorneys, and that if such communications were inadvertently collected (or inadvertently identified from more general searches), they may not be

²⁸ Memorandum from E. J. Holland, Jr., HHS Assistant Secretary for Administration, to HHS Operating Division and Staff Division Heads, "Policy for Monitoring Employee Use of HHS IT Resources" (June 26, 2013). The June 2013 HHS directive states that although the IT warning banner—which states that the employee consents to having no reasonable expectation of privacy regarding any communication or data transiting or stored on the HHS IT system and that the employee understands that the Department may monitor the use of HHS IT resources for lawful government purposes—gives the OPDIVs the authority to monitor employee use of IT resources, "it is each

shared with a non-law-enforcement party who requested the monitoring, or anyone else, without express written authorization from the Office of General Counsel (OGC) and other appropriate Department officials.

In September 2013, as FDA's COO, I proposed a Staff Manual Guide (SMG) establishing interim policies and procedures that will strengthen the Agency's ability to effectively document, analyze, authorize, and manage requests to monitor use of HHS and FDA IT systems and resources. Among other things, this proposed SMG would: (1) provide standards for when employee computer monitoring may take place; (2) establish a Review Committee, consisting of a representative from FDA's OCC, 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, to review requests for monitoring and to develop procedures for such review; (3) state that requests for computer monitoring shall be narrowly tailored in time, scope, and degree of monitoring; (4) require that all requests to monitor shall identify the least-invasive approach to accomplish the monitoring objectives, and that when reviewing requests for monitoring, authorizing officials shall also consider whether there are alternative information-gathering methods available that can be utilized to address the potential risk, without jeopardizing the Agency's objectives; (5) provide standards for documenting written authorizations for computer monitoring; and (6) state that no computer monitoring authorized or conducted may target communications with law enforcement entities, the OSC, members of Congress or their staff, employee union officials, or private attorneys. FDA is currently in the

OPDIV's responsibility to carry out monitoring in a fashion that protects employee interests and ensures the need for monitoring has been thoroughly vetted and documented."

process of developing processes and procedures to fully implement the HHS policy on computer monitoring.

CONCLUSION

In accordance with Federal law, and in order to ensure that FDA can effectively carry out its mission, the Agency must be vigilant to protect against the misuse or unauthorized disclosure of the confidential information that is regularly entrusted to it. FDA believes that the policies and procedures that HHS and the Agency have put in place appropriately and effectively balance the individual interests of employees and the critical need to safeguard the security and integrity of the data and information systems that FDA has been entrusted to manage.

Thank you for your commitment to the mission of FDA and for the opportunity to testify today about issues related to the monitoring of FDA employees' use of Agency IT resources. I am happy to answer any questions you may have.

Chairman ISSA. Ms. Canterbury?

STATEMENT OF ANGELA CANTERBURY

Ms. CANTERBURY. Thank you.

And good day, Chairman Issa, Ranking Member Cummings, members of the committee.

The FDA spied on whistleblowers, which set off a firestorm that led us to this hearing today. But the public story of whistleblowers began in 2008, when FDA physicians and scientists warned Congress, and shortly thereafter the President, that the process for approving medical devices was broken, allowing potentially ineffective and unsafe products to be marketed. And as Senator Grassley noted, there has long been problems with bureaucrats at the FDA respecting the scientific process.

The report released today by Chairman Issa and Senator Grassley and the HHS IG report document how FDA surveillance of whistleblowers was reckless and heedless of legal limits and whistleblower protections. Certainly security concerns and available technology will outstrip constitutional rights and whistleblower protections unless Congress works to balance those goals.

To be frank, we question why FDA should be in the surveillance business in the first place. The FDA's mission is to ensure our food and drugs and devices are safe.

Any suspicion of unlawful disclosures of information or criminal misconduct should be investigated by law enforcement. Federal agencies cannot be allowed to police themselves. That is why we have IGs, the OSC, the FBI, and Congress.

Ms. CANTERBURY. Even with just cause and proper controls, it will be difficult, if not impossible, to protect whistleblowers if agencies are allowed to gather electronic evidence without limits or oversight. And to what end? The Issa-Grassley report shows the leaks of confidential information to the press were not confirmed by this pervasive, invasive electronic surveillance. And so, as with the NSA domestic surveillance, the risks to our rights may be greater than the ability of surveillance to protect against risks to security, much less claims of harm to trade secrets or harm to profits.

No doubt the FDA is in a tough spot: attempting to put into place a process that is more proscribed for surveillance critics, but also placating the lawyers for drug and device companies that demand that information be kept confidential. Needless to say, the FDA does not have it right yet. Rather than protect whistleblowers from unwarranted FDA surveillance, its interim policy protects the FDA from whistleblowers. It shields it from accountability. Nothing in the FDA's interim policy would prevent FDA managers from using information collected by the surveillance as retaliation for whistleblowing. Thus, this policy does little to lift the chilling effect that fosters wrongdoing. How can the FDA ensure the public's health and safety if the scientists and physicians are too afraid to come over when deadly mistakes are made?

And far too many mistakes are made. Inadequately tested metal-on-metal hip replacements cause crippling disability. Defective cardiac defibrillators, unclean syringes containing deadly bacteria, old-fashioned pediatric feeding tubes cause fatalities because they lack the well-known, inexpensive safeguard. And these are just the

medical devices that the FDA allowed on the market, not to mention the food and drug approval disasters.

And if the FDA isn't doing its job and lives are at risk, we have to ask why. The FDA whistleblowers warned us that corners were being cut and scientists were being overruled by the bureaucrats.

We need whistleblowers. However, it is worth noting that throughout Mr. Harris' testimony there was no acknowledgment of the public interest in protecting whistleblowers, only of employee protections, yet it is well known that whistleblowers save lives and taxpayer dollars and are among the best partners in crime fighting. Congress protected public whistleblowing so that waste, fraud, and abuse, and threats to public health and safety would be known.

As Senator Grassley said, you couldn't do the majority of the oversight this body does without whistleblowers and without the media, but the FDA policies do nothing to encourage or safeguard public whistleblowing, which is protected so long as the disclosure of information is not prohibited under law. They claim to exclude from surveillance in their interim policy the targeting of disclosures to Congress, the OSC, and others, but this is not enough. A legal review at the front end will not prevent legal public whistleblowing collected through spying from falling into the hands of those in a position to retaliate.

Clearly, the FDA and other agencies will not get this right on their own. Congress and the President must mandate a government-wide policy to prevent future surveillance abuses. Of course, interfering with communications to Congress and retaliating for whistleblowing is already against the law, and there are some protections for the identities of whistleblowers in other laws, but Congress should consider specifically protecting the identity of a whistleblower in any surveillance that is done by an agency.

Today, we don't nearly know enough about the scope of surveillance across the government. I encourage you to order a report, a study looking at this issue. I encourage you to conduct oversight over other concerns with national security and insider threat programs that might threaten whistleblowers. But importantly, we must not forget what brought us here today, which is the FDA whistleblowers. They were concerned about the device approval process they believed might put lives at risk.

FDA officials should not be held accountable for approving—they should be held accountable for approving ineffective and unsafe products, and flawed devices must be taken off the market. There must be more transparency and less deference to the demands for confidentiality by drug and device companies. Seriously, I wonder how much time and taxpayer dollars is spent protecting so-called confidential commercial information.

Finally, please do all you can to ensure that FDA managers are held accountable for any violations of the rights of the scientists and physicians who sought to make medical devices more safe and more effective. Thank you.

Chairman ISSA. Thank you.

[Prepared statement of Ms. Canterbury follows:]



**Testimony by Angela Canterbury, Director of Public Policy,
Project On Government Oversight,
before the House Oversight and Government Reform Committee regarding
“Limitless Surveillance at the FDA: Protecting the Rights of Federal Whistleblowers”
February 26, 2014**

Chairman Issa, Ranking Member Cummings, and Members of the Committee, thank you for your oversight of protections for whistleblowers and for inviting me to testify today.

I am the Director of Public Policy at the Project On Government Oversight (POGO). Founded in 1981, POGO is a nonpartisan independent watchdog that champions good government reforms. POGO’s investigations into corruption, misconduct, and conflicts of interest achieve a more effective, accountable, open, and ethical federal government. Thus, POGO has a keen interest in protecting whistleblowers who assist in uncovering and deterring government waste, fraud, abuse, mismanagement, and threats to public health and safety.

Today I also am speaking as a member of the steering committee of the Make It Safe Coalition, a nonpartisan, trans-ideological network of organizations dedicated to strengthening protections for public and private sector whistleblowers. More than 400 groups have endorsed our efforts to strengthen whistleblower legislation, on behalf of millions of Americans.¹ Our coalition is deeply concerned with how surveillance of government and federal contractor employees threatens civil service rights, whistleblower protections, and taxpayer accountability.

The Food and Drug Administration (FDA) spied on whistleblowers—resulting in this hearing after significant media attention, statements and letters from concerned members of Congress, reports by my organization, lawsuits, and investigations by the Office of Special Counsel, the Health and Human Services (HHS) Inspector General, as well as the staff report for Chairman Issa and Senator Grassley, anticipated to be released in conjunction with this hearing.

The FDA Whistleblowers

The history of contention between FDA whistleblowers and the agency has been well documented. Thus, I will not delve into every detail, but instead will summarize and then highlight some of the more important facts. FDA physicians and scientists made whistleblower disclosures of their reasonable belief that the process for approving medical devices was broken, allowing potentially ineffective and unsafe products to be marketed. At a minimum, this resulted

¹ Open letter from Project On Government Oversight et al., to President Barack Obama and Members of the 111th Congress, regarding strong and comprehensive whistleblower rights, September 23, 2011. www.makeitsafecampaign.org/wp-content/uploads/2013/11/WPA-Sign-On-Letter.pdf (Downloaded November 15, 2013)

in reprisal for whistleblowing, allegations of leaks of confidential information, and inappropriate surveillance of FDA whistleblowers by the FDA—basically, a federal maelstrom of misconduct.

On October 14, 2008, a group of eight FDA physicians and scientists wrote to Representative John Dingell, then-Chairman of the House Committee on Energy and Commerce,² as reported by *The New York Times* about five weeks later.³ In the letter, the whistleblowers described serious wrongdoing by mid-level and senior FDA officials involved in approving medical devices before they are marketed through the 510(k) program. Specifically, the whistleblowers stated that managers in the FDA's Center for Devices and Radiological Health (CDRH) had "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."

The whistleblowers also asserted that "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 [and] . . . 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."

The FDA whistleblowers also stated that when physicians and scientists objected to these practices by CDRH managers, the managers engaged in reprisals. The whistleblowers stated that they had then contacted top FDA officials, including FDA Commissioner Andrew von Eschenbach, but following this there was little or no change in the practices of CDRH managers. The writers concluded their letter to Representative Dingell: "As the Branch of government responsible for oversight of the FDA, we urgently seek your intervention and help."

Energy and Commerce Chairman Dingell and Subcommittee on Oversight and Investigations Chairman Bart Stupak subsequently wrote to FDA Commissioner von Eschenbach on November 17, 2008, summarizing the statements of the FDA employees and reviewing some of the federal laws on retaliation against whistleblowers.⁴

On January 7, 2009, the FDA whistleblowers wrote to John Podesta, head of the Obama presidential transition team, raising these concerns and listing medical devices that the FDA had

² Letter from FDA Whistleblowers to Representative John Dingell, regarding misconduct by FDA managers at the Center for Devices and Radiological Health, October 14, 2008.

[http://www.lasikcomplications.com/CDRHscientists\(Oct08\).pdf](http://www.lasikcomplications.com/CDRHscientists(Oct08).pdf) (Downloaded February 24, 2014)

³ Gardiner Harris, "F.D.A. Scientists Accuse Agency Officials of Misconduct," *The New York Times*, November 17, 2008. http://www.nytimes.com/2008/11/18/health/policy/18fda.html?_r=0 (Downloaded February 24, 2014)

⁴ Letter from Representative John Dingell, Chairman of the Committee on Energy and Commerce and Representative Bart Stupak, Chairman of the Subcommittee on Oversight and Investigations, to the Honorable Andrew von Eschenbach, Commissioner of the U.S. Food and Drug Administration, regarding the FDA whistleblowers and federal whistleblower laws, November 17, 2008. <http://www.pharmamedtechbi.com/~media/A3A72512AC214BDFAF7979622DCFA28C> (Downloaded February 24, 2014)

approved for marketing over the whistleblowers' objection that there was a lack of sufficient evidence of efficacy or safety—an objection that they had expressed to the managers.⁵ For example, the scientists had objected to the FDA approval process for computer-aided detection devices (CAD) used in breast and colon cancer detection because the scientists considered them not to be safe or effective. The FDA whistleblowers wrote a similar letter to President Obama on April 2, 2009.⁶

On January 15, 2009, Senator Grassley sent a letter to FDA Commissioner von Eschenbach echoing the concerns of the whistleblowers and emphasizing the right of the whistleblowers to communicate with Congress without interference.⁷

In February 2009, POGO issued a report authored by Dr. Ned Feder that additionally exposed misconduct and flaws in the medical device approval process.⁸ Based on internal FDA documents obtained by POGO, *The FDA's Deadly Gamble with the Safety of Medical Devices* shows that senior FDA officials in CDRH decided not to enforce a regulation—the Good Laboratory regulation or GLP—that helps protect patients from unsafe devices. The officials did this over the protests of CDRH scientists. Our report describes this and other serious problems in the FDA.

There was considerable coverage of the whistleblowing in print and broadcast media.⁹ Some reports referred to the group of FDA scientists and physicians as the FDA whistleblowers or as the “FDA Nine.”¹⁰ On March 13, 2009, FDA employees received an email from FDA Acting Commissioner Frank Torti informing them that “FDA must comply with its obligations to keep certain information in its possession confidential. . . . Violation of these provisions can result in

⁵ Letter from FDA Whistleblowers to John Podesta, Presidential Transition Team, regarding concerns and objections about FDA approved medical devices, January 7, 2009. <http://www.whistleblowers.org/storage/whistleblowers/documents/FDAwhistleblowers/letter2transitionteam.pdf> (Downloaded February 24, 2014)

⁶ Letter from FDA Whistleblowers to President Barack Obama, regarding their concerns about FDA misconduct, April 2, 2009. <http://www.finance.senate.gov/imo/media/doc/prg040209a.pdf> (Downloaded February 24, 2014)

⁷ Letter from Senator Charles Grassley, Ranking Member Committee on Finance, to Honorable Andrew von Eschenbach, Commissioner of the U.S. Food and Drug Administration, regarding FDA whistleblowers and the right to communicate with Congress, January 15, 2009. <http://www.grassley.senate.gov/about/upload/FDA.pdf> (Downloaded February 25, 2014)

⁸ Project On Government Oversight, *The FDA's Deadly Gamble with the Safety of Medical Devices*, February 18, 2009. <http://www.pogo.org/our-work/reports/2009/ph-fda-20090218.html>

⁹ “FDA scientists allege mismanagement at agency,” January 9, 2009. Video clip. Accessed February 24, 2014.

CNN.com. <http://www.cnn.com/2009/POLITICS/01/09/fda.scientists/#cnnSTCVideo> (Downloaded February 24, 2014); Ricardo Alonso-Zaldivar, “FDA scientists complain to Obama of ‘corruption,’” *The Associated Press*, January 8, 2009. http://www.foxnews.com/printer_friendly_wires/2009Jan08/0,4675,FDADissidents,00.html (Downloaded February 24, 2014); Alicia Mundy and Jared A. Favole, “FDA Scientists Ask Obama to Restructure Drug Agency,” *The Wall Street Journal*, January 8, 2009.

<http://online.wsj.com/news/articles/SB123142562104564381> (Downloaded February 24, 2014); Gardiner Harris, “In F.D.A. Files, Claims of Rush to Approve Devices,” *The New York Times*, January 12, 2009.

http://www.nytimes.com/2009/01/13/health/policy/13fda.html?_r=1& (Downloaded February 24, 2014)

¹⁰ Some of the whistleblowers were federal employees, and others were contractors. And the number of whistleblowers has changed over time—now there are only five seeking justice in court.

disciplinary sanctions and/or individual criminal liability.”¹¹ Senator Grassley shot back with letter to Torti stating, “If the memo sent last week was intended to have a chilling effect on FDA employees who want to speak up about problems, then that memo is contrary to the President’s call for open and transparent government, and the Acting Commissioner needs to set the record straight.”¹²

FDA Surveillance of the Whistleblowers

It isn’t clear exactly when it began, but the FDA admits that it conducted a secret surveillance program to monitor the whistleblowers’ emails and other computer-generated documents.¹³ The FDA claims the surveillance was in response to the unauthorized disclosure of confidential commercial information to journalists in 2009 and 2010. The targets were the individuals known to have blown the whistle in letters to Congress, President Obama, and the President’s Transition Team.

On April 21, 2010, the FDA received a request from the legal counsel for GE Healthcare, Inc. that the FDA investigate how information GE Healthcare considered a trade secret had appeared in a *Times* article on March 28, 2010.¹⁴ The article included statements by two of the FDA whistleblowers.

Incredibly, the CDRH managers claim that it was in response to that letter that they began to use spyware on April 22, 2010, to conduct surveillance on one of the scientists quoted in the article¹⁵—which was only one day after the letter was received.¹⁶ Instead of going to the HHS IG prior to beginning the investigation, as required by HHS procedures,¹⁷ CDRH managers

¹¹ Frank Torti, Acting Commissioner of Food and Drugs, e-mail message to FDA employees, “Re: Protecting Confidential Information,” March 13, 2009. <http://online.wsj.com/public/resources/documents/wsj090317-Tortimemo.pdf> (Downloaded February 25, 2014)

¹² Senator Chuck Grassley of Iowa, “Grassley works to protect FDA whistleblowers,” March 24, 2009. http://www.grassley.senate.gov/news/Article.cfm?customel_dataPageID_1502=19930 (Downloaded February 25, 2014)

¹³ Letter from Jeanne Ireland, Assistant Commissioner for Legislation at the Food and Drug Administration, to Senator Charles Grassley, Ranking Member of the Committee on the Judiciary, regarding information about the FDA’s use of computer monitoring, July 13, 2012. <http://www.grassley.senate.gov/about/upload/FDA-7-13-12-agency-response-to-Grassley-regarding-email-surveillance-on-eve-of-NYT-story.pdf> (Downloaded February 24, 2014) (Hereinafter Letter from Jeanne Ireland, Assistant Commissioner for Legislation at the Food and Drug Administration)

¹⁴ Gardiner Harris “Scientists Say F.D.A. Ignored Radiation Warnings,” *The New York Times*, March 28, 2010. http://www.nytimes.com/2010/03/29/health/policy/29fda.html?_r=0 (Downloaded February 24, 2014)

¹⁵ Letter from Jeanne Ireland, Assistant Commissioner for Legislation at the Food and Drug Administration, p. 3.

¹⁶ Kimberly Holden, Assistant Commissioner for Management at the Food and Drug Administration, e-mail message to Horace Coleman and Mark McCormack, “FW: Advice/Investigation,” April 23, 2010. <http://pogoarchives.org/m/wi/holden-emails-to-coleman-20100423.pdf> (Downloaded February 25, 2014)

¹⁷ The HHS manual states in part:

“A. In order to provide objective uniform procedures for the handling of allegations of wrongdoing covered by this chapter, it shall be the responsibility of the Office of Inspector General (OIG) to investigate allegations of wrongdoing reported to the OIG or to refer such allegations to the appropriate operating division (OPDIV), the appropriate staff division (STAFFDIV), to Assistant Secretary for Administration and Management (ASAM), to another law enforcement agency, or to another appropriate authority.

requested that the Office of Internal Affairs (OIA) investigate “unauthorized disclosure of information.”¹⁸ The OIA rightly referred the matter to HHS IG in order to “remove any potential allegations of impartiality.”

HHS IG declined to investigate on May 18, 2010 in a letter stating:

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.¹⁹

Perhaps the CDRH managers improperly took matters into their hands because the HHS IG had declined a request by the FDA Commissioner’s Office to investigate an earlier alleged unauthorized disclosures related to the FDA whistleblowers’ whistleblowing in late 2008 and early 2009.²⁰ On March 26, 2009, then-FDA Assistant Commissioner William McConagha made a referral to HHS OIG after having received a letter of complaint from the attorney of device maker iCAD.

In any case, the CDRH managers spent the coming months spying on the FDA whistleblowers. Once they thought they had collected evidence of criminal violations, CDRH Director Dr. Jeffrey Shuren, requested an HHS IG investigation.

Again, HHS IG declined to investigate the alleged unauthorized disclosures by the whistleblowers, but first consulted with the Department of Justice to determine if there was evidence of a criminal violation. DOJ declined to prosecute, and HHS IG closed the case with a November 15, 2010, declination letter to the Director of CDRH, which states:

B. Every employee, supervisor, and management official shall report any allegations of criminal offenses he/she receives, immediately to the OIG, unless it is clear to him/her that the allegation is frivolous and has no basis in fact.” . . .

D. Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to a supervisor, management official, or the OIG.” Department of Health and Human Services, “General Administration Manual Chapter 5-10: Procedures for Reporting Misconduct and Criminal Offenses,” December 26, 2006. http://www.hhs.gov/hhsmanuals/gam/chapters/5-10_rev.pdf (Downloaded February 25, 2014)

¹⁸ Mark McCormack, Office of Internal Affairs at the Food and Drug Administration, “Case Initiation and Fact Sheet,” May 14, 2010. <http://pogoarchives.org/m/wi/fda-oia-ci-and-fact-sheet-20140423.pdf> (Downloaded February 25, 2014)

¹⁹ Letter from Scott Vantrease, Assistant Special Agent in Charge, Special Investigations Branch of the Food and Drug Administration Office of the Inspector General, to Mark McCormack, Special Agent in Charge, regarding the decision not to investigate allegations of leaks, May 18, 2010. www.kkc.com/files/oigletter_fdawbdisclosuresprotected.pdf (Downloaded February 24, 2014)

²⁰ Letter from William McConagha, Assistant Commissioner for Integrity and Accountability, Department of Health and Human Services, to Scott Vantrease, Director of the Special Investigations Unit at the Department of Health and Human Services Office of Inspector General, regarding referring allegations of misconduct for a formal investigation, March 26, 2009. <http://pogoarchives.org/m/wi/mcconagha-2nd-referral-hhs-oig-re-icad-20090326.pdf>

Your office indicated it had developed sufficient evidence to address the misconduct through administrative process, and as such, no further action will be taken by the OIG.²¹

But instead of taking disciplinary action through an administrative process, CDRH managers continued their unauthorized spying on the whistleblowers.

This initially narrow surveillance quickly expanded into what *The New York Times* called, “a much broader campaign to counter outside critics of the agency’s medical review process.”²² A program called Spector 360 was used to take screenshots “every five seconds, all e-mails sent or received on the laptops, all data stored on or printed from the computers, all keystrokes performed, and data stored on personal thumb drives attached to the computers.” Documents were cataloged in 66 huge directories reportedly containing more than 80,000 pages of computer documents culled from what must have been millions of data viewed by contractors hired by the CDRH managers to conduct the surveillance.

Swept up in the dragnet were whistleblower disclosures to congressional staff, the Office of Special Counsel, and my organization, the Project On Government Oversight.

On January 15, 2012, the FDA Whistleblowers filed a lawsuit claiming violations of their rights under the First, Fourth, and Fifth Amendments.²³

Interestingly, none of this may have come to light if the documents captured in the surveillance had not been reportedly posted online by an FDA contractor.²⁴ *The Washington Post* reported that among the trove of FDA documents found to have been posted online, there were “Copies of the e-mails show that, starting in January 2009, the FDA intercepted communications with congressional staffers and draft versions of whistleblower complaints complete with editing notes in the margins.”²⁵

The revelations of the surveillance set off a firestorm that led to this hearing today.²⁶ Naturally, Senator Grassley was incensed by the surveillance of the whistleblowers, having already warned

²¹ Letter from Scott Vantrease, Assistant Special Agent in Charge, Special Investigations Branch of the Food and Drug Administration Office of the Inspector General, to Jeffrey Shuren, Director of the Center for Devices and Radiological Health, regarding alleged misconduct by the FDA whistleblowers, November 15, 2010. <http://pogoarchives.org/m/wi/vantrease-20101115.pdf> (Downloaded February 24, 2014)

²² Eric Lichtblau and Scott Shane, “Vast F.D.A. Effort Tracked E-Mails of Its Scientists,” *The New York Times*, July 14, 2012. <http://www.nytimes.com/2012/07/15/us/fda-surveillance-of-scientists-spread-to-outside-critics.html?page-wanted=all> (Downloaded February 24, 2014) (Hereinafter “Vast F.D.A. Effort Tracked E-Mails of Its Scientists”)

²³ *Hardy v. Shuren*, No. 1:11-cv-01739 (D. D.C. filed Sept. 28, 2011) [Second Amended Complaint filed July 17, 2012] <http://epic.org/amicus/fda/hardy/Hardy-v-Shuren-2nd-Complaint.pdf> (Downloaded February 25, 2014)

²⁴ “Vast F.D.A. Effort Tracked E-Mails of Its Scientists”

²⁵ Ellen Nakashima and Lisa Rein, “FDA staffers sue agency over surveillance of personal e-mail,” *The Washington Post*, January 29, 2012. http://www.washingtonpost.com/world/national-security/fda-staffers-sue-agency-over-surveillance-of-personal-e-mail/2012/01/23/gIQAj34DbQ_story.html (Downloaded February 24, 2014)

²⁶ Ellen Nakashima and Lisa Rein, “FDA lawyers authorized spying on agency’s employees, senator says,” *The Washington Post*, July 16, 2012. http://articles.washingtonpost.com/2012-07-16/politics/35489846_1_enca-

the FDA to uphold legal protections for the whistleblowers.²⁷ On January 31, 2012, Senator Grassley sent the FDA Commissioner yet another strongly-worded letter pointing out that interfering with communications to Congress is a violation of the law.²⁸ He told *The New York Times* that agency officials “have absolutely no business reading the private e-mails of their employees. They think they can be the Gestapo and do anything they want.”²⁹

Representative Chris Van Hollen said, “It is absolutely unacceptable for the FDA to be spying on employees who reach out to members of Congress to expose abuses or wrongdoing in government agencies.”³⁰ Investigations were begun or expanded by Senator Grassley, Chairman Issa, the HHS IG, and the OSC.

In two memos circulated together on June 20, 2012, the President’s Office of Management and Budget (OMB) and the OSC directed all agencies to “evaluate their monitoring policies and practices, and take appropriate steps to ensure that those policies and practices do not interfere with or chill employees’ use of appropriate channels to disclose wrongdoing.”³¹ However, the FDA has not yet done so.

Unanswered Questions

It is not yet known whether the FDA whistleblowers will get the justice they seek or whether FDA managers will be held accountable for retaliation. The whistleblowers’ lawsuit is still pending, as is the OSC’s investigation into retaliation. Though the HHS IG did not investigate the alleged leaks of confidential information, the IG twice reviewed the claims of retaliation by the whistleblowers and did not substantiate retaliation.³² However, POGO has long been

[jefferson-fda-contractor-computer-surveillance](#) (Downloaded March 4, 2013) (Hereinafter “FDA lawyers authorized spying on agency’s employees, senator says”)

²⁷ “FDA lawyers authorized spying on agency’s employees, senator says”

²⁸ Letter from Senator Charles Grassley, Ranking Member of the Committee on the Judiciary, to the Honorable Margaret Hamburg, Commissioner of the Food and Drug Administration, regarding the agency’s treatment of whistleblowers, January 31, 2012. <http://pogoarchives.org/m/wi/ceg-to-fda-whistleblower-20120131.pdf>

²⁹ “Vast F.D.A. Effort Tracked E-Mails of Its Scientists,”

³⁰ Jason Lange, Andy Sullivan and Anna Yukhananov, “FDA surveillance operation draws criticism from lawmakers,” July 15, 2012. http://articles.chicagotribune.com/2012-07-15/news/sns-rt-us-usa-fda-lawmakersbre86e0gx-20120715_1_fda-medical-devices-surveillance (Downloaded February 24, 2014)

³¹ Memorandum from Steven VanRoekel, Federal Chief Information Officer and Boris Bershteyn, General Counsel, to the Chief Information Officers and General Counsels, regarding Office of Special Counsel Memo on Agency Monitoring Policies and Confidential Whistleblower Disclosures, June 20, 2012. <http://www.whistleblowers.org/storage/whistleblowers/documents/ombandosc.monitoringmemo.pdf> (Downloaded March 4, 2013)

³² Investigative Memorandum from Elton Malone, Special Agent in Charge, Special Investigations Branch, Department of Health and Human Services Office of Inspector General, to Unknown FDA Employees, regarding closing the investigation, October 14, 2010. <http://pogoarchives.org/m/wi/oig-memo-no-prohibited-practices-20101014.pdf> (Hereinafter Investigative Memorandum from Elton Malone); Investigative Memorandum from Elton Malone, Special Agent in Charge, Special Investigations Branch, Department of Health and Human Services Office of Inspector General, to Unknown FDA Employees, regarding closing the investigation, February 4, 2010. <http://pogoarchives.org/m/wi/oig-memo-prohibited-personnel-practices-20100204.pdf>; Letter from Timothy Menke, Deputy Inspector General for Investigations Department of Health and Human Services Office of Inspector General, to Joshua Sharfstein, Principal Deputy Commissioner Department of Health and Human Services, regarding the status of the OIG investigation, February 23, 2010. <http://pogoarchives.org/m/wi/oig-letter-re-mgmt-wrongdoing-20100223.pdf>.

concerned that the two reviews were conducted improperly.³³ The first HHS IG investigation focused on criminal wrongdoing, instead of non-criminal retaliation for whistleblowing. And, from our January 2011 letter to FDA Commission Margaret Hamburg regarding the second investigation:

The Office of Investigations did not conduct a new investigation, but instead initiated a “Special Inquiry.” According to the Investigative Memorandum of October 2010, the findings of the Special Inquiry were based on the “case file and all reports and evidence contained therein”—in other words, the findings of the recent Special Inquiry in September 2010 were based exclusively or almost exclusively on documentation gathered during the 2009 investigation. But the 2009 investigation was looking for the wrong things: criminal violations rather than administrative wrongdoing (i.e. alleged violations of FDA regulations and whistleblower retaliation).

Also still in question is whether the FDA medical device approval process has improved at all. Have the concerns raised in the first place by the FDA whistleblowers about ineffective and dangerous devices been adequately addressed?

In August of 2010, CDRH responded to the substance of whistleblowing by issuing an action plan and requesting an independent review of the troubled 510(k) program.³⁴ CDRH asked the Institute of Medicine (IOM) to conduct this review, and IOM determined the 510(k) program should be scrapped and replaced with an integrated premarket and post-market regulatory framework.³⁵ The IOM report states:

510(k) clearance is not a determination that the cleared device is safe or effective. The committee concludes that the 510(k) process lacks the legal basis to be a reliable premarket screen of the safety and effectiveness of moderate-risk devices and, furthermore, that it cannot be transformed into one.

The CDRH ignored this recommendation and continued the program.

In the 510(k) process, the whistleblowers objected to management overruling the scientists’ and physicians’ recommendations that the FDA should not approve a particular device for marketing. The FDA has regulations, including 21 CFR 10.70, describing clearly what must happen when

³³ Letter from Project On Government Oversight, to the Honorable Kathleen Sebelius, Secretary of the U.S. Department of Health and Human Services, regarding the FDA’s negligent oversight of unsafe medical devices, January 12, 2011. <http://www.pogo.org/our-work/letters/2011/ph-fda-20110112.html> (Hereinafter Letter regarding the FDA’s negligent oversight of unsafe medical devices)

³⁴ Steve Strong, “The Ever-Changing Regulatory Environment,” Minnetronix http://www.minnetronix.com/partials/company-industry_insights-single/the-ever-changing-regulatory-environment/ (Downloaded February 24, 2014)

³⁵ Institute of Medicine of the National Academies, *Medical Devices and the Public’s Health: The FDA 510(k) Clearance Process at 35 Years*, July 29, 2011. <http://www.iom.edu/~media/Files/Report%20Files/2011/Medical-Devices-and-the-Publics-Health-The-FDA-510k-Clearance-Process-at-35-Years/510k%20Clearance%20Process%202011%20Report%20Brief.pdf> (Downloaded February 24, 2014)

there are “significant controversies or differences of opinion” over decisions.³⁶ However, managers violated these regulations, and the result was the marketing of devices that are unsafe or ineffective. POGO has repeatedly asked for more oversight to ensure that efficacy and public health and safety are the priorities in medical device approvals.³⁷

The HHS IG has initiated investigations into FDA’s internal controls and quality review for 510(K) device approval process and CDRH’s policies for resolving scientific disputes.³⁸

Undeniable: The FDA’s Improper Employee Surveillance

What is evident is that the FDA acted improperly in its surveillance of FDA whistleblowers. There is wide agreement that at a minimum the FDA improperly conducted employee surveillance and jeopardized whistleblower and privacy protections.

In addition, the FDA’s employee surveillance does not appear to have been effective as an investigative tool for the stated purpose. But employee surveillance is a handy tool for those seeking to chill whistleblowing and retaliate against whistleblowers. As with the NSA domestic surveillance, the risks to the rights of those under surveillance seem to outweigh the enhancements to security.

What’s at Stake?

Lives are at stake. The FDA’s problems can be deadly. There have been far too many ineffective and unsafe medical devices approved by the broken agency:

- Inadequately tested metal-on-metal hip replacements caused a crippling, hard-to-treat disability.³⁹
- Defective cardiac defibrillators worked well when first implanted, but later some of them suddenly failed.⁴⁰
- Unclean syringes containing deadly bacteria caused serious and sometimes fatal infections.⁴¹

³⁶ 21 CFR 10.70, “Documentation of significant decisions in administrative file,” <http://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol1/pdf/CFR-2012-title21-vol1-sec10-70.pdf> (Downloaded February 25, 2014)

³⁷ Letter from Project On Government Oversight, to Gerry Roy, Deputy Inspector General for Investigations, Office of Investigations at the Department of Health and Human Services, regarding FDA’s CDRH’s low standard of medical devices approval, September 28, 2010. <http://www.pogo.org/our-work/letters/2010/ph-fda-20100928-1.html>; Letter regarding the FDA’s negligent oversight of unsafe medical devices; Project On Government Oversight, “Obama Administration Should Re-Open Investigation of FDA Wrongdoing After Inspector General Office Rejected Whistleblower Complaints,” January 13, 2011. <http://www.pogo.org/about/press-room/releases/2011/ph-fda-20100113.html#sthash.KODITW4a.5Ev9Gx9g.dpuf>

³⁸ Investigative Memorandum from Elton Malone

³⁹ Gregory Curfman and Rita Redberg, “Medical Devices—Balancing Regulation and Innovation,” *New England Journal of Medicine*, Vol. 365, September 15, 2011, pp. 975-977.

<http://www.nejm.org/doi/full/10.1056/NEJMp1109094> (Downloaded February 25, 2014)

⁴⁰ William H. Maisel, “Semper Fidelis—Consumer Protection for Patients with Implanted Medical Devices,” *New England Journal of Medicine*, Vol. 358, March 6, 2008, pp. 985-987.

<http://www.nejm.org/doi/full/10.1056/NEJMp0800495> (Downloaded February 25, 2014)

- Old-fashioned pediatric feeding tubes caused fatalities because they lacked a well-known, inexpensive safeguard that precludes accidental infusion of pureed baby food directly into the baby's bloodstream.⁴²

And this is just medical devices. The FDA has also failed to contain deadly food contamination outbreaks⁴³ and have allowed dangerous drugs⁴⁴ on the market. The FDA isn't doing its job and lives are at risk; and we have to ask: Why?⁴⁵

Whistleblowers are the guardians of the public trust and safety. Without proper controls at FDA and throughout the government, employee surveillance is a serious threat to whistleblower protections. The resulting chilling effect will significantly reduce accountability—thus keeping waste, fraud, abuse, and threats to public health and safety in the shadows. Whistleblowers also are among the best partners in crime-fighting. It is a well-known fact that whistleblowers have saved countless lives and billions of taxpayer dollars.

A survey conducted in 2012 by the Association of Certified Fraud Examiners found that nearly half of occupational fraud cases were uncovered by a tip or complaint from an employee,

⁴¹ Christina Jewett, "Could FDA Have Prevented Syringe Deaths?" *ProPublica*, February 26, 2009.

<http://www.propublica.org/article/could-fda-have-prevented-in-syringe-deaths> (Downloaded February 25, 2014)

⁴² Gardiner Harris, "U.S. Inaction Lets Look-Alike Tubes Kill Patients," *The New York Times*, August 20, 2010.

<http://www.nytimes.com/2010/08/21/health/policy/21tubes.html?pagewanted=all> (Downloaded February 25, 2014)

The fatalities can be prevented completely by a requirement that the feeding tube have a connector incompatible with connectors for intravenous fluids; See also: Associated Press, "Is the FDA a broken agency?" March 3, 2009, <http://www.today.com/id/29495269/43136851%20In%20the%20five%20years%20since%20the%20AP%20article%20was%20published,%20more%20disasters%20have%20occurred.#.UwzmEONdW4I> (Downloaded February 25, 2014) (Hereinafter "Is the FDA a broken agency?"); POGO summarized the story of some of these disasters: Ned Feder, "Powerful Leader Takes Command of a Battered FDA: Irresistible Force Meets Immovable Object," May 19, 2009. <http://www.pogo.org/about/press-room/releases/2009/ph-fda-20090519.html> (Hereinafter "Powerful Leader Takes Command of a Battered FDA: Irresistible Force Meets Immovable Object"); Letter from Danielle Brian and Ned Feder, Project On Government Oversight, to Kathleen Sebelius, Secretary, U.S. Department of Health and Human Services, regarding reinvestigating FDA's negligent oversight of unsafe medical devices, January 12, 2011. <http://www.pogo.org/our-work/letters/2011/ph-fda-20110112.html> (Hereinafter Letter from Danielle Brian and Ned Feder, Project On Government Oversight, to Kathleen Sebelius)

⁴³ Salmonella-infected peanut butter: Centers for Disease Control and Prevention, "Multistate Outbreak of *Salmonella* Bredeney Infections Linked to Peanut Butter Manufactured By Sunland, Inc. (Final Update)," November 30, 2012. <http://www.cdc.gov/salmonella/bredeney-09-12/> (Downloaded February 25, 2014); Listeria-infected cantaloupes: Centers for Disease Control and Prevention, "Investigation Update: Multistate Outbreak of Listeriosis Linked to Whole Cantaloupes from Jensen Farms, Colorado," October 25, 2011. <http://www.cdc.gov/listeria/outbreaks/cantaloupes-jensen-farms/102511/index.html> (Downloaded February 25, 2014)

⁴⁴ Fungus-contaminated steroid mixture: Centers for Disease Control and Prevention, "Multistate Outbreak of Fungal Meningitis and Other Infections," October 23, 2013. <http://www.cdc.gov/hai/outbreaks/meningitis.html> (Downloaded February 25, 2014); Heparin: Gardiner Harris, "U.S. Identifies Tainted Heparin in 11 Countries," *The New York Times*, April 22, 2008. <http://www.nytimes.com/2008/04/22/health/policy/22fda.html?pagewanted=all> (Downloaded February 25, 2014)

⁴⁵ "Is the FDA a broken agency?"; "Powerful Leader Takes Command of a Battered FDA: Irresistible Force Meets Immovable Object"; Letter from Danielle Brian and Ned Feder, Project On Government Oversight, to Kathleen Sebelius.

customer, vendor, or other source.⁴⁶ In the case of fraud perpetrated by owners and executives, more than half were uncovered by tips from whistleblowers. A 2011 academic study confirmed that whistleblowers play a bigger role than external auditors, government regulators, self-regulatory organizations, or the media in detecting fraud.⁴⁷

But perhaps the best illustration of how whistleblowers can save taxpayer dollars is the more than \$38 billion recovered since 1987 through the hugely successful False Claims Act (FCA), championed by Senator Grassley.⁴⁸

The FCA prohibits a person or entity from fraudulently or dishonestly obtaining or using government funds. The law not only acts as a deterrent, but also incentivizes whistleblowing through the financial awards and strong protections against retaliation.⁴⁹ Federal Circuit Court Judge Kenneth Keller Hall said that the FCA provisions supplement the government's "regular troops" since it "let loose a posse of ad hoc deputies to uncover and prosecute frauds against the government."⁵⁰

But unfortunately, the cost-benefit analysis for most whistleblowing is so often all cost to the whistleblower and all benefit to society. Professor Richard E. Moberly in his testimony before Congress aptly stated:

Furthermore, almost all the benefits of a whistleblower's disclosure go to people other than the whistleblower: society as a whole benefits from increased safety, better health, and more efficient law enforcement. However, most of the costs fall on the whistleblower. There is an enormous public gain if whistleblowers can be encouraged to come forward by reducing the costs they must endure. An obvious, but important, part of reducing whistleblowers' costs involves protecting them from retaliation after they disclose misconduct.⁵¹

Whistleblowing works for the public, but not without strong protections for the whistleblower. Recognizing this, Congress has repeatedly strengthened the rights and procedures available to whistleblowers. In 2012, Chairman Issa and Ranking Member Cummings—along with

⁴⁶ Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud & Abuse: 2012 Global Fraud Study*, 2012, pp. 14-19. http://www.acfe.com/uploadedFiles/ACFE_Website/Content/ttrn/2012-report-to-nations.pdf (Downloaded February 20, 2014)

⁴⁷ Alexander Dyck, Adair Morse, and Luigi Zingales, "Who Blows the Whistle on Corporate Fraud?" <http://www.afajof.org/afa/forthcoming/4820p.pdf> (Downloaded May 10, 2011)

⁴⁸ Department of Justice, Office of Public Affairs, "Fraud Statistics – Overview: October 1, 1987 - September 30, 2013," December 23, 2013. http://www.justice.gov/civil/docs_forms/C-FRAUDS_FCA_Statistics.pdf (Downloaded February 20, 2014)

⁴⁹ 31 U.S.C. § 3730, "Civil actions for false claims." <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title31/pdf/USCODE-2011-title31-subtitleIII-chap37-subchapIII-sec3730.pdf> (Downloaded February 25, 2014)

⁵⁰ *United States ex rel. Milam v. Univ. of Tex. M.D. Anderson Cancer Ctr.*, 961 F.2d 46, 49 (4th Cir. 1992), paragraph 17. <http://law.justia.com/cases/federal/appellate-courts/F2/961/46/208412/> (Downloaded February 20, 2014)

⁵¹ Testimony of Richard E. Moberly, Professor, before the Committee on Education and Labor, Subcommittee on Workforce Protections, One Hundred Tenth Congress, on "Private Sector Whistleblowers: Are There Sufficient Legal Protections?" May 15, 2007, p. 35. <http://www.gpo.gov/fdsys/pkg/CHRG-110hrg35185/pdf/CHRG-110hrg35185.pdf> (Downloaded December 1, 2011)

Representative Van Hollen, then-Representative Platts, and their Senate colleagues—championed the latest enhancements to federal employee protections with the enactment of the Whistleblower Protection Enhancement Act.⁵² While these reforms go a long way to improve the prospects for whistleblowing on government wrongdoing, employee surveillance, left unaddressed, seriously undermines these and other statutory protections for whistleblowers that Congress intended.

An Opportunity for Reform

This committee's attention to the unacceptable actions of the managers at FDA will hopefully serve as a catalyst for government-wide reforms. Certainly security concerns and available technology will outstrip the protection of civil liberties, whistleblower protections, and other constitutional rights unless there is a concerted effort to consider all of these goals together. We can and should move towards a better policy and to ensure more accountability now. But if left to their own devices, the agencies cannot be expected to get this right.

The FDA and other agencies should not be in the surveillance or law enforcement business. Federal agencies cannot be allowed to police themselves—that is why we have IGs, the OSC, DoJ, and Congress.

Investigations of unauthorized, illegal disclosures of information and other criminal misconduct must be conducted by law enforcement investigators—such as the FBI or the Inspectors General—not bureaucrats. While we acknowledge there may be a *very* limited need for agencies to gather evidence of wrongdoing by employees when there is reasonable suspicion of non-criminal misconduct, the electronic surveillance is ripe for abuse—as demonstrated by the FDA. Even with just cause and proper controls, it will be difficult, if not impossible to ensure constitutional rights are not violated.

To what end? As with the NSA domestic surveillance, the risks to our rights may be greater than the ability of the surveillance to protect against risks to security.

On September 12, 2012, FDA Commissioner Hamburg issued a memorandum directing the Chief Information Officer (CIO) and Chief Counsel to “promptly develop a written procedure” for employee surveillance that includes some safeguards (Hamburg Memo).⁵³ Presumably, that written procedure is embodied in the interim policies and procedures established last September by the FDA in its Staff Manual Guide (Interim Policy).⁵⁴ No doubt the FDA is in a tough spot,

⁵² Project On Government Oversight et al., “After a Campaign Waged Over More Than a Decade, the Whistleblower Protection Enhancement Act Becomes Law,” December 3, 2012. <http://www.pogo.org/about/press-room/releases/2012/20121203-advocates-laud-president-whistleblower-reforms.html>

⁵³ Memorandum from Margaret Hamburg, Commissioner of the Food and Drug Administration, to Walter Harris, Chief Operating Officer, Eric Perakslis, Chief Information Officer, and Elizabeth Dickinson, Chief Counsel of the Food and Drug Administration, regarding developing a written procedure for employee surveillance, September 24, 2012. <http://pogoarchives.org/m/wi/hamburg-memo-20120924.pdf> (Hereinafter Memorandum from Margaret Hamburg)

⁵⁴ Walter Harris, Deputy Commissioner for Operations, Chief Operating Officer at the Department of Health and Human Services, “Monitoring of Use of HHS/FDA IT Resources,” September 26, 2013. <http://pogoarchives.org/m/wi/interim-monitoring-policy-20130926.pdf>

attempting to put into place a process that is more proscribed for surveillance critics, but also placating the lawyers for drug and device companies that demand that information be kept confidential.

Needless to say, the FDA doesn't have it right yet.

Nothing in this policy would prevent the FDA Commissioner or Chief Operating Officer from using information collected by the surveillance as retaliation for whistleblowing or providing it to others who might. The policy does little to lift the chilling effect at FDA that fosters waste, fraud, abuse, and threats to public health and safety. How can the FDA ensure the public's health and safety if scientists and physicians are too afraid to come forward when deadly mistakes are made?

Instead, the interim policy would allow the FDA managers to control a vast and far-reaching surveillance program without any oversight from an independent outside entity. Rather than protect whistleblowers from unwarranted FDA surveillance, this policy protects the FDA from whistleblowers and shields it from accountability.

Simply stating that the FDA will follow existing laws to protect whistleblowers is not enough—the procedures do not build in strong, substantive safeguards. The Interim Policy does attempt to protect some sensitive communications by prohibiting the targeting of communications with law enforcement, the OSC, members of Congress or their staff, employee union officials, or private attorneys. However, it does not include a similar prohibition on other protected disclosures—most notably, *public whistleblowing*, which is protected as long as the disclosure of the information is not prohibited under law.

Congress protected public whistleblowing because we live in a democracy that relies on an informed public and freedom of the press. In numerous instances, threats to public health and safety, waste, fraud, and abuse and other wrongdoing would never have come to light or been addressed without public whistleblowing.⁵⁵

The FDA has not ensured employees, contractors, and grantees can exercise *all* of their legal rights without fear of retaliation. Thus, any final policy must prohibit specifically monitoring communications with *anyone* that may include a protected disclosure. According to the Whistleblower Protection Act, these communications would include a reasonable belief that the disclosure evidences “any 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.”⁵⁶

In practice, it may be difficult, if not impossible, to prevent the inadvertent capture of protected disclosures while monitoring employee communications. Therefore, any final policy must

⁵⁵ David Shuster, “Whistle-blowers who made their mark,” NBC News, June 2, 2005. http://www.nbcnews.com/id/8076349/ns/msnbc-hardball_with_chris_matthews/t/whistle-blowers-who-made-their-mark/#.UwuAnuNdWSo (Downloaded February 24, 2014)

⁵⁶ 5 U.S.C. §2302, “Merit system principles,” <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partIII-subpartA-chap23.pdf> (Downloaded February 25, 2014)

mandate a legal review and express authorization before any potentially protected communication that is collected is shared. Notification of potential legal pitfalls to recipients of collected information, as called for in the Hamburg Memo, is woefully insufficient.⁵⁷

The FDA must do more to ensure all agency personnel and federal fund recipients are better trained in whistleblower protections. Under the WPA, it is the responsibility of the head of each agency, in consultation with the Office of Special Counsel, to ensure that agency employees are informed of the rights and remedies available to them under the Whistleblower Protection Act.⁵⁸ The OSC, has a certification program which allows agencies to demonstrate that they have fulfilled this legal obligation. Last year, only three agencies sought and received certification—and, remarkably, the FDA was not one of them.⁵⁹ Clearly, certification should not be voluntary.

Last December, in its second National Action Plan for the Open Government Partnership, the Obama Administration committed to taking steps over the next two years with the stated goal of strengthening and expanding protections for federal whistleblowers.⁶⁰ These commitments include mandating participation in the Office of Special Counsel's Whistleblower Certification Program. However, Congress should ensure that agency compliance with the WPA notification requirement and certification will continue into the future by putting the requirement into statute.

Federal contractors and grantees also are required to notify their employees of the whistleblower protections available to them.⁶¹ There should be a mechanism to certify this compliance as well. Perhaps this could be part of the contracting or grant-making process, or the Whistleblower Ombudsmen in the Offices of Inspectors General could play a role. The Inspectors General have responsibilities to conduct investigations of claims of retaliation by contractor and grantee employees, as well as by national security and intelligence community workers.⁶² Agencies are currently certifying compliance with Presidential Policy Directive 19, which protects national security and intelligence community whistleblowers. These certifications should be made public, but so far only the Department of Defense has done so.

⁵⁷ Memorandum from Margaret Hamburg

⁵⁸ 5 U.S.C. §2302(c), "In administering the provisions of this chapter," <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partIII-subpartA-chap23.pdf> (Downloaded February 25, 2014)

⁵⁹ U.S. Office of Special Counsel, "Agencies That Have Completed the 2302(C) Certification Program," September 20, 2013. <http://osc.gov/outreach/AgenciesCertified.htm> (Downloaded February 24, 2014)

⁶⁰ The U.S. White House, *The Open Government Partnership Second Open Government National Action Plan for the United States of America*, December 5, 2013. http://www.whitehouse.gov/sites/default/files/docs/us_national_action_plan_6p.pdf (Downloaded February 24, 2014)

⁶¹ 10 USC § 2409, "Contractor employees: protection from reprisal for disclosure of certain information," <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap141-sec2409.pdf> (Downloaded February 25, 2014) (Hereinafter 10 USC § 2409); 41 U.S. Code § 4712, "Pilot program for enhancement of contractor protection from reprisal for disclosure of certain information," <http://uscode.house.gov/view.xhtml?jsessionid=809F5786EE28C3E4FA53851870F5F683?req=granuleid%3AUSC-2012-title41-chapter47&saved=%7CZ3JhbnVsZWlkOlVTOy0vMDEyLXRpdGxINDEtc2VjdGlvbjQ3MTI%3D%7CcdHlJlZXNvbnQ%3D%7C%7C0%7Cfalse%7C2012&edition=2012> (Downloaded February 25, 2014) (Hereinafter 41 U.S. Code § 4712)

⁶² President Barack Obama, "Presidential Policy Directive/PPD-19: Protecting Whistleblowers with Access to Classified Information," October 10, 2012. <http://www.pogoarchives.org/m/wi/white-house-10-10-12.pdf>

Additionally, a memo and staff manual guide will not alone ensure that privacy, whistleblower, and civil service rights are protected in employee surveillance. The policies and procedures for safeguarding employee rights whenever investigations or surveillance is conducted should include penalties for violations and should have the force of law. Therefore, a permanent regulation for all of HSS—not just the FDA—would be most appropriate.

However, there ought to be a government-wide approach. The Department of Justice has the appropriate legal expertise for developing such policy, in consultation with the OSC and MSPB. Moreover, the FDA is only attempting to write a policy ad hoc because of all the unwanted attention it's receiving. But what is to prevent other agencies from spying on employees without regard to the legal rights of these employees? Congress and/or the President must mandate a government-wide policy to protect whistleblower and other constitutional rights and prevent future abuses.

Of course, interfering with communications to Congress⁶³ and retaliating for whistleblowing⁶⁴ is against the law. Although the law does protect the identity of whistleblowers in other ways—the OSC and IG are prohibited from disclosing the identity of whistleblowers except in certain circumstances⁶⁵—there is little to prevent other agencies from identifying whistleblowers by collecting communications. Congress should consider amending the WPA and contractor protections to specifically prohibit an agency from using collected communications to identify a whistleblower.

Today, we don't know nearly enough about the scope of employee surveillance across the government. We hope that this committee will order a comprehensive study of how agencies are currently conducting surveillance of employees while protecting their rights. Far more needs to be known about current practices, legal protections, effectiveness, and cost. A government-wide study by the Government Accountability Office (GAO) and/or the Merit Systems Protection Board (MSPB) would provide the executive branch and Congress with a more complete picture and recommendations for best-practice policies.⁶⁶

⁶³ 18 USC § 1505, "Obstruction of proceedings before departments, agencies, and committees," <http://www.law.cornell.edu/uscode/text/18/1505> (Downloaded February 25, 2014); 5 USC § 7211, "Employees' right to petition Congress," <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partIII-subpartF-chap72.pdf> (Downloaded February 25, 2014)

⁶⁴ 5 USC § Section 2302, "Prohibited personnel practices," <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partIII-subpartA-chap23.pdf> (Downloaded February 25, 2014); 10 USC § 2409; 41 USC § 4712.

⁶⁵ 5 USC § 1213(h), "Provisions relating to disclosures of violations of law, gross mismanagement, and certain other matters," <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title5/pdf/USCODE-2011-title5-partIII-chap12-subchap11-sec1213.pdf> (Downloaded February 25, 2014); 5 USC App. Section 7(b), "Protects employees who file complaints or provide information to the Inspector General," <http://statecodesfiles.justia.com/us/2011/title-5/appendix-title-5/1350/section-7/document.pdf> (Downloaded February 25, 2014)

⁶⁶ While GAO might be more effective at auditing current agency surveillance practices, given the technical components, the MSPB may be well-suited to use that information to develop recommendations on protecting the merit system. The mission of the MSPB is to "Protect the Merit System Principles and promote an effective Federal workforce free of Prohibited Personnel Practices." "U.S. Merit Systems Protection Board," <http://www.mspb.gov/> (Downloaded February 24, 2014)

Naturally, there also must be a different approach with the ever-growing intelligence and national security workforce. More and more of the federal workforce is labeled as national security sensitive—and there is a jaw-dropping lack of oversight. The number of people cleared for access to classified information reached a record high in 2012, soaring to more than 4.9 million.⁶⁷ Add to that untold numbers of civil servants and contractors without access to classified information, but in positions labeled as national security sensitive.⁶⁸ In order to prevent leaks of classified information, it is critical that there are truly safe channels for legal disclosures.

We have long been concerned about the potential for abuse of whistleblowers as a result of Insider Threat programs mandated by the President and Congress.⁶⁹ The program pits employees against one another,⁷⁰ creating an atmosphere of suspicion and intimidation likely to silence would-be whistleblowers. Intended to protect national security, implementation of the Insider Threat Program at agencies that have little to do with national security issues suggests a serious overreach. Blurring the line between spies and whistleblowers can only harm national security. An investigation by McClatchy last year discovered that agencies were using the Insider Threat Program as grounds to pursue unauthorized disclosures of unclassified information—information that whistleblowers can legally disclose to anyone under current law.⁷¹

We hope this committee will also conduct rigorous oversight of whistleblower protections for the national security and intelligence community workforce.

Importantly, we must not lose sight of what brought us here today. Scientists at the FDA were concerned about a device approval process that they believed might put lives at risk. We urge you to ensure that the critical work being done by the CDRH puts the public's health and safety first. Bureaucrats at FDA should not be allowed to overrule the findings of expert scientists and physicians, except under extraordinary circumstances. There are no criminal penalties for FDA officials who allow unsafe devices to be approved. FDA officials should be held accountable for approving ineffective or unsafe products, and flawed devices must be taken off the market. There must be far more transparency and less deference to the demands for confidentiality by the drug and device companies.

⁶⁷ Office of the Director of National Intelligence, 2012 Report on Security Clearance Determinations, January 2013, p. 3. <http://www.dni.gov/files/documents/2012%20Report%20on%20Security%20Clearance%20Determinations%20Final.pdf> (Downloaded November 14, 2013)

⁶⁸ We only know from the government's brief in *Conyers* that there are at least half a million workers in positions labeled as national security sensitive at the Department of Defense (DoD) alone: *Kaplan v. Conyers*, Initial Brief for Director, Office of Personnel Management, November 23, 2011, p. 4, n. 7. <http://mspbwatch.files.wordpress.com/2012/08/berry-conyers-initialbriefforopm.pdf> (Downloaded November 14, 2013) (Hereinafter *Kaplan v. Conyers* Initial Brief for OPM Director)

⁶⁹ The White House, "Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011 <http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-> (Downloaded February 24, 2014)

⁷⁰ Defense Security Service, Counterintelligence Directorate, "INSIDER THREATS: Combating the ENEMY within your organization," <http://www.dss.mil/documents/ci/Insider-Threats.pdf> (Downloaded February 24, 2014)

⁷¹ Marisa Taylor and Jonathan Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," McClatchyDC, June 20, 2013. <http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html#.Uccv--vmVHl> (Downloaded February 24, 2014)

Finally, please do all you can to ensure the FDA whistleblowers get the justice that they deserve and that FDA managers are held accountable for any violations of the rights of the scientists and physicians who sought to make medical devices safer and more effective.

Thank you for the opportunity to testify before you today. POGO and the Make It Safe Coalition pledge to continue to work with you to fulfill the promise of a government that is truly open and accountable to the American people.

I look forward to your questions.

Chairman ISSA. Mr. Harris, a couple of questions. First of all, I mentioned you'd be the person that would review a request to spy on an employee in the future, you would be the first point of contact. Is that correct?

Mr. HARRIS. Yes, sir.

Chairman ISSA. Okay. And your degree is in business administration?

Mr. HARRIS. Can you repeat the question?

Chairman ISSA. You have an MBA?

Mr. HARRIS. Yes, sir, I do.

Chairman ISSA. You're not a lawyer?

Mr. HARRIS. I'm not.

Chairman ISSA. And the person that you, once you decided to do it, that you'd go to, would be the same person, the general counsel, who approved the spying in the past. Is that correct?

Mr. HARRIS. Well, I want to give the committee accurate information, so most of what we speak about today predates my tenure at FDA.

Chairman ISSA. No, no, I understand. I'm just looking at the process.

Mr. HARRIS. Right.

Chairman ISSA. The process in place, the so-called protection that the agency has put forward is you'd still go to the same general counsel. The first lawyer, if you will, would be the lawyer who thought this was just fine before, which is the general counsel, and second of all, before that, you'd go to the chief operating officer, who is, by definition, probably not an attorney.

Mr. HARRIS. That's right.

Chairman ISSA. Okay. I just want to understand the system because I don't approve of it.

Mr. HARRIS. I'll give you the process. So we have a process that requires a request to be formally written.

Chairman ISSA. No, no. I apologize. But I only have 3 minutes and 55 seconds, and to be honest, the process sucks. So now let's move on.

Ms. Canterbury, you said it very well. They had suspected a criminal activity. Is that correct?

Ms. CANTERBURY. They suspected that confidential information—

Chairman ISSA. Right. So alleging—

Ms. CANTERBURY. —was disclosed.

Chairman ISSA. Right. So alleging the criminal activity, they did not go to the IG, they did not go to the criminal investigation units of which there are a multitude within—HHS has their own, obviously the FBI.

Let me ask a question, Mr. Harris. Your opening statement, you used some very carefully toned words, and I picked up on just a couple of them as another nonlawyer with a business degree. You said that you didn't target or use a term like that of Members of Congress, but you didn't protect, in other words—not you—but the general counsel received all of the information without any attempt to screen out, you know, Mr. Van Hollen or my committees or Senator Grassley's committees or for that matter, lawyers, doctors, there was no protection in place.

Mr. HARRIS. Again, Mr. Chairman, that predates my time at FDA.

Chairman ISSA. Right. But I just want to make sure that's correct, that there was no protection put in place. So the idea that you didn't target doesn't really matter. You didn't protect the likelihood of five known whistleblowers, and especially Dr. Smith, a known whistleblower, the likelihood is he's still talking to Members of Congress, he's still—he didn't change his opinion that the FDA had problems. So by definition, the FDA knowingly intercepted correspondence with Members of Congress because there was a reasonable expectation that he was having correspondence with Members of Congress.

Let me just ask a couple of quick questions. To your knowledge, you weren't there at the time, there were five people targeted. Was there anybody else at the FDA that had access to the information that was linked to The New York Times? Anyone else?

Mr. HARRIS. Again, that predates my time at FDA.

Chairman ISSA. Well, why don't we make the assumption that there were just a load of them, that these five people were by all reasonable account not the only ones that had the ability to have gotten this information.

Since you received none, the real question is, did the FDA and does the FDA have not the ability to be narrow, but the ability to be broad? If you have a leak and 4,000 people could have leaked it, the only way to do it properly would be to make the assumption that you had to equally monitor 4,000, unless you had a specific, credible reason to believe that one person had done it. Isn't that right? You're the approving officer. I need to understand how you would do it.

Mr. HARRIS. In the current process, we would ask for a written request. That request would then be reviewed by a committee before we make any actions happen. From the committee, it goes to a legal review, and we get—

Chairman ISSA. You're the final approval. Would you have targeted just these five known whistleblowers or would you have had to target more people who had accessed that information?

Mr. HARRIS. It depends on the scenario.

Chairman ISSA. Okay. So you're not binding yourself to any kind of protection for the Federal workforce from being targeted.

Mr. HARRIS. Just the opposite, Chairman. We clearly state in all documents these days, since our new policy has been implemented, that we consider interactions with the Hill, legal counsel, OMB, et cetera, as protected activities. When our staff has any interaction with that type of information, they know to—

Chairman ISSA. Oh, your staff.

Mr. HARRIS. Any staff.

Chairman ISSA. Oh, no, no. But the whole point is, who gets to see this information under your current policy first?

Mr. HARRIS. Under the current policy, the information comes immediately back to me. I then bring the appropriate folks to the table. We talk through our next steps. It goes no further.

Chairman ISSA. Okay. So you're looking at correspondence that they had with me and you're going to protect me.

Mr. HARRIS. No. No. What I'm doing is actually when they walk up on that type of information, they cease—

Chairman ISSA. Who is they?

Mr. HARRIS. Those who are actually—

Chairman ISSA. Who are they?

Mr. HARRIS. Those staff members who are part of the process.

Chairman ISSA. Okay. I just want to understand. You've got staff members looking at correspondence with Members of Congress.

Mr. HARRIS. No, sir.

Chairman ISSA. Well, you just said that.

Mr. HARRIS. That was not my statement. My statement was, when we are going through the monitoring process, should my staff who is actually administering the monitoring process find information of that type is considered protective activity.

Chairman ISSA. But they see it in order to consider it.

Mr. HARRIS. They do stop—well, you know, during the monitoring process they may walk up on that, but they stop all processes today. I can't tell you what happened 2 or 3 years ago, but I can tell you what happens today.

Chairman ISSA. Okay. Well, let me just close by saying do you know the name "Paul Hardy"?

Mr. HARRIS. I do.

Chairman ISSA. Do you know what happens if you Google his name?

Mr. HARRIS. No, sir. What happens?

Chairman ISSA. Well, he Googled his name because he was concerned and apparently looking for a job, feeling that his was insecure.

Mr. HARRIS. Oh, I'm sorry. I thought you said Paul Harvey.

Chairman ISSA. No, Hardy.

Mr. HARRIS. No, I don't know Paul Hardy.

Chairman ISSA. Well, he was one of the targets, and the Internet was filled and Google-able with all those screen shots basically, because your agency took no precautions on that confidential information, his correspondence with Congress, if it was there, his correspondence with his doctor, his lawyer, his priest, anybody. And it simply became an Internet phenomenon that you could Google and get it because it was put out on an open site because the FDA did not take the precautions, did not fill out the forms properly, and did not protect that information which it had captured clandestinely. Isn't that true?

Mr. HARRIS. Well, that may have been the case a few years ago.

Chairman ISSA. No, no, no, wait a second. You're a witness, you're under oath.

Mr. HARRIS. I am, sir.

Chairman ISSA. You say may have been the case. Are you here today and you don't know if it was the case?

Mr. HARRIS. I was not there 2 years ago, so I would not have—

Chairman ISSA. Do any of you know if it was the case or if I'm just coming up with something that's Internet lore?

Ms. CANTERBURY. Respectfully, sir, I believe that Dr. Shuren was in charge of CDRH at the time.

Chairman ISSA. Are you familiar with the—and I'm just on the same thing, I've got to give time to the ranking member—but are

you familiar with the release of that information, the fact that it wasn't protected, and it became essentially Internet public?

Dr. SHUREN. Yes, I know information was made public. I don't know the full extent of it. I wasn't involved in dealing with the contractor or any handling of that material. But I am aware that information was posted on the Internet.

Chairman ISSA. Okay. And I'll give you equal time, but if I had your indulgence for one more quick question.

There has been an alluding to the confidential information The New York Times got. Just for the record, it wasn't patent information. It wasn't a deep, dark secret on how you make a product. It was the fact the product was in question as to whether it was safe and effective. Isn't that correct, Doctor?

Dr. SHUREN. It was whether or not the product was under review, and that has been considered confidential. Companies many times do not want competitors to know that they're working on a product and that it's under review by the agency.

Chairman ISSA. Okay. I just want to understand. The level of trade secret is a product, The New York Times reported, was under review and may not have been safe.

Dr. SHUREN. It was just simply that the product was under review would be confidential commercial information.

Chairman ISSA. Okay. But it's something that—I want everyone to understand that the term “confidential” is not the term the public thinks is all that confidential. Most people look at these products, clinical trials, the process of approval, and then the question of whether they're being re-reviewed, most people probably listening and watching today believe the public has a right to know that information and may not agree with the FDA's view that that is private or confidential or somehow a secret from the American people as to whether a product that may or may not yet be on the market is safe and effective.

Ms. Canterbury, if you wanted to respond quickly.

Ms. CANTERBURY. I couldn't agree more. I think that at the base of all of these questions is, why is this information considered confidential in the first place, and is that serving the public health and safety? I think that there needs to be a question answered about why the FDA did not choose to first verify whether or not it was legitimately considered to be confidential in the first place and investigate that matter instead of investigating a so-called leak of confidential information.

Chairman ISSA. Thank you.

Mr. Cummings.

Dr. SHUREN. If I may. I was going to respond to your question.

Chairman ISSA. Of course.

Dr. SHUREN. But our employees know that that information is confidential, and that has been for longstanding time. Keeping that information confidential is critically important. It can undermine ongoing review of medical device applications. In fact, I believe in that particular case it, in fact, did that. It undermines our medical device program, keeping that confidential information confidential. Companies, that information we need for making decisions about products, and companies rely on the fact that we protect that information. We don't protect it, the companies don't bring innovative

technologies to the U.S., our patients lose. Public health gets hurt when that happens. That's why those protections are in place in the first place. That's why Congress put the protections in place. And it hurts American businesses—

Chairman ISSA. Doctor, I appreciate what you're saying. They bring innovative products here because of profit. But let's understand one thing. Do these companies sign a gag order, are they prohibited from disclosing that you're looking at it?

Dr. SHUREN. No, they may disclose it. That is their decision to make. It's their information.

Chairman ISSA. Okay. Thank you. It's a one-way gag order.

Please, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

I want to pick up where the chairman left off. Dr. Shuren, prior to the initiation of the monitoring, the agency believed that the FDA employees were involved in unauthorized disclosures of confidential information and trade secrets as a result of the monitoring. What did the agency find?

Dr. SHUREN. So the agency did find, as I understand that, there was unauthorized disclosures to members of the public, and that is, from our perspective, in violation of HHS personnel policy and probably a violation of the law.

Mr. CUMMINGS. So the agency found clear evidence that Dr. Smith and the other FDA employees whose computers were monitored were involved in unauthorized disclosures of confidential agency information. And as I understand it, that's a violation of the law and can be subject to criminal penalties. Is that correct?

Dr. SHUREN. Depending upon the kind of information that's released. But, yes, this can be violative of the law.

Mr. CUMMINGS. Now, when I listen to Ms. Canterbury—and I'm going to come back to you in a moment, Ms. Canterbury—you know, one of things that she said was perhaps the FBI and other agencies should be handling these kinds of issues. And I'm trying to figure out how would even—and you can address this in a minute—I mean, you all have laws that we passed that you're trying to adhere to. And so, I guess there's almost a—there is a duty to at least look into it. Is that right?

Dr. SHUREN. There is an obligation to look into it.

Mr. CUMMINGS. And if you don't look into it, then you're in trouble. Is that right?

Dr. SHUREN. That's correct.

Mr. CUMMINGS. And as I understand it, with regard to The New York Times, there were people who were—companies that were complaining that, look, you know, we gave you information, we expected it not to be—not to read about it in The Times. That's the last place we expected it to be. We thought it was confidential. And now this is where we see it. Is that fair to say?

Dr. SHUREN. That is correct. Actually, the company involved sent a complaint and actually pointed out that we were in violation of Federal law. They asked for an internal investigation. Five days after receipt of that letter is when monitoring was started. It was also in the setting of a pattern of unauthorized disclosures that had occurred starting over a year before.

Mr. CUMMINGS. Now, I don't know whether you—you need to hear this question, too, Mr. Harris—I don't know whether you heard me a little bit earlier, but it seems that there is a major issue here with regard to whether this investigation should have been just retrospective or retrospective and prospective. And I'm just wondering what's your view on that.

Dr. SHUREN. So the honest answer is, I don't know. I'm not an IT expert. And when the issue was raised what we asked for, what I asked my executive officer for was options to try to identify the source of the leak and to address further unauthorized disclosures. Our information technology people decided on what the appropriate solution would be. So I do not have the expertise.

Mr. CUMMINGS. So you just passed it on, look, you said we got a—obviously The New York Times has got information that they're not supposed to have, I just want you to help me figure out how this information is getting out there. Is that one of the things you wanted to know?

Dr. SHUREN. Yes, what the source of the leak was, what the options were for doing it. And they proceeded to authorize—

Mr. CUMMINGS. And what was your plan after you got this information? I mean, what happened?

Dr. SHUREN. So what happened with the information, we put a process in place; also tried to protect privacy. First the IT people collected information they thought met very narrow search terms. That information was then put on secure iron keys, one of two. It was passed to my executive officer. It was then conveyed to a subject matter expert to look at, was there confidential information in here? And then if there are issues of concern, there was something I called the management team. There was a group set up, which was the assistant commissioner for management, it was lawyers from HHS and employment law, and it was people from our labor employee relations, a group already established actually as in part as a protection for these complainants. And that information then went up to these individuals and others to try to decide what, if there is an issue here, what are the appropriate steps to take, which could be administrative or could be referred on for other action.

Mr. CUMMINGS. And do you know which specific medical devices these individuals were concerned about?

Dr. SHUREN. I know of some that were reported out in the press and some that went on a referral up to the OIG. And I say that because I wasn't a subject matter expert, and I'm not the person who makes the personnel decision, so I was not reviewing the emails. We were trying to limit the people who would look at any information coming out in order to respect privacy of the individuals.

Mr. CUMMINGS. Now, have these employee safety concerns been borne out? So you don't know that either? In your assessment, were their concerns valid?

Dr. SHUREN. Well, for the products—and I am aware of the concerns that they were raising on a variety of products, and I don't think that their concerns were valid. I'll raise the case in question here of The New York Times article of CT colonography, which was to be used to screen asymptomatic patients for cancer. And there

was a lot of good evidence on the table, several clinical studies, a big one that was funded by the Federal Government. And just last year, we held a joint meeting of two advisory committees at the FDA, experts in radiology and gastroenterology, 20 people in all, and they unanimously felt that CT colonography should remain an option for the screening of asymptomatic patients.

Mr. CUMMINGS. Well, it's interesting that the employees raised concerns regarding integrity of the device review process, and they called it corrupted and distorted. Did you know that?

Dr. SHUREN. Yes.

Mr. CUMMINGS. And when you first took over the center, did you evaluate these concerns regarding the review process?

Dr. SHUREN. I did look into the concerns from my own standpoint of the complainants. The Office of the Inspector General was also investigating whether or not managers were retaliating against these complainants. And I will tell you the OIG found that there was no retaliation, there was no prohibitive personnel practices. The complainants raised concerns about that investigation, they reopened it, and then they subsequently concluded again there had been no retaliation.

I will tell you I also took steps along the way for trying to assure that these complainants were actually protected and to make sure that if there really were problems and if I thought there were problems, I would have done something about it.

Mr. CUMMINGS. And so you're telling us today under sworn testimony that you are concerned about whistleblowers and would do everything in your power to protect them?

Dr. SHUREN. Yes, I would. One example of something that I did do soon after I got there, I was hearing concerns from them, I was looking into the managers, I did not see problems. But I said to them, look, you're complaining about the managers all the way up your chain of command to the office director. Here is what I will do. I have two offices involved in premarket review. I will offer to move the entire Radiological Devices Branch out of the one office and move it to a new office with new managers.

I didn't have evidence that I had bad managers. The OIG was continuing its investigation. But I said, in light of that, if the OIG finds problems, we will pursue that. But I am willing to do this. I am willing to disrupt my organization because of your concerns. And I did that. They wanted the move. I made the move. And within a few weeks of the move, the exact same complaints were now being levied against a brand new group of managers.

Mr. CUMMINGS. Ms. Canterbury, you heard Mr. Harris, and he talked about the IG report. I guess that was what he was saying, the recommendations have now—

Mr. HARRIS. Yes, sir.

Mr. CUMMINGS. You are telling us, Mr. Harris, that all of those recommendations are now in place?

Mr. HARRIS. Yes, they are.

Mr. CUMMINGS. And when did they go in place?

Mr. HARRIS. September of last year.

Mr. CUMMINGS. September of last year. So with regard to the recommendations, you all didn't know about them in September, did you?

Mr. HARRIS. No.

Mr. CUMMINGS. We just got the report last night.

Mr. HARRIS. Correct.

Mr. CUMMINGS. So, how did, I mean, how did that come about, just out of curiosity?

Mr. HARRIS. Again, it goes back to I documented a couple of notes in Ms. Canterbury's statements about making sure we protect all employees and their rights. She's right on the money. So our process does that.

I got a little bit concerned with the chairman's comment that the process may suck. So the reason we're here is because they were not commonly understood across the agency. So what we put in place today are commonly understood processes where a request comes in, it's formally documented, it then goes before a committee, and then goes for a legal review and approval. Even beyond that, if we approve a process for monitoring to begin, there are regular checkpoints along the way to make sure we know what's going on there.

So we weren't aware of the IG's report, but, you know, we could have taken this in a Keystone Kop approach and then find ourselves here on a regular basis. We decided to look at a more methodical approach to this, and knowing that there are many scenarios out there that we have consider when putting any policy like this in play. What I want to have us do is have the folks who operate within the administrative process, when it comes to monitoring, understand the processes first, then we permeate the organization so they can understand what procedures we go through.

Mr. CUMMINGS. Ms. Canterbury, just in my last question. You have your concerns. You heard Mr. Shuren say that he's very concerned. It sounds like Mr. Harris is very concerned and taken steps to address the issue. Do you believe that it's been adequately addressed?

Ms. CANTERBURY. Thank you, sir. I believe that they are taking steps. I don't believe it's been adequately addressed. I would very much like to hear how he intends to protect the public whistleblowing once he receives, as COO, what has been collected. And there is no legal review of the collected information guaranteed under the interim rules, and I would like to hear from him on that.

I also think it's curious that Dr. Shuren said that he sought to protect those particular whistleblowers who were targeted for surveillance. If that's his idea of protection, I find that very curious.

I also want to point out that it doesn't matter if the whistleblowers' concerns bear out to be valid, whether those devices are unsafe or effective. As you know, sir, it is a reasonable belief that is protected under law for whistleblowing.

And I also wanted to just point out another curious thing that Dr. Shuren said, which was the surveillance began 5 days after the receipt of a letter from GE Healthcare. In fact, the letter is dated April 16th. They received the letter on April 21st, and the surveillance began on April 22nd, according to documents that we have through FOIA and through the IG report and through the staff committee report. So I have never in my life, sir, seen the Federal Government move that fast. I find it highly suspect that the letter

arrived and then they made the decision after the arrival of the letter to do this surveillance.

Mr. CUMMINGS. Well, Ms. Canterbury, my time has run out. This is what this is all about, trying to make sure that the Federal Government is doing the right thing. But I want to keep in mind what Mr. Shuren did say. He's saying he's got a set of laws that we passed, and he's trying to adhere to the laws that we passed, and so there are certain things that they had to do. The question is, did they do it right? I don't think so. But it sounds like they're going in the right direction.

Unfortunately, I've run out of time. I wish Mr. Harris could answer your question, but I've run out of time, and I'll yield back.

Mr. FARENTHOLD. [Presiding] Thank you very much, Mr. Cummings.

We'll now recognize the gentleman from Michigan for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman, and thanks to the witnesses for being here today.

Dr. Shuren, I'll give you a chance to respond to the timeline that Ms. Canterbury addressed here. It appears the differences in the dates of beginning the investigation, sending the letters, respond to that, if you would, please.

Dr. SHUREN. Yes. No, in terms of when we received it, it was close, and my only point was, it was still within 5 days of getting the receipt of that letter the monitoring started. Mainly to say that this was not disconnected in time, that this was related to this complaint that came in, as well as a series of unauthorized complaints. That was my only point to make.

Mr. WALBERG. Ms. Canterbury, let me ask you some questions, and then you might respond to that with greater detail as well. Is there any situation where monitoring employee communications with Congress or OSC can be justified?

Ms. CANTERBURY. No.

Mr. WALBERG. It's a simple answer. Then is the problem of monitoring protected employee communications widespread across the Federal agencies?

Ms. CANTERBURY. I don't know—

Mr. WALBERG. Federal agencies.

Ms. CANTERBURY. Yeah, I don't know the answer to that, and I don't know that anyone does. I think that it would be very good for this committee to order a study, a comprehensive independent study, perhaps at GAO, perhaps in consultation with the MSPB to determine the extent to which agencies are using surveillance programs on their employees.

Mr. WALBERG. So this could be widespread?

Ms. CANTERBURY. It very well could be, and there could be widespread abuses.

Mr. WALBERG. What protections can agencies put in place to minimize the monitoring of protected communications such as with Congress or OSC?

Ms. CANTERBURY. Well, firstly, I think that we need to question whether or not there is a legitimate reason for agencies to use surveillance on questions of criminal behavior or leaks of potentially unlawfully disclosed information. I think that, again, law enforcement should be conducting those investigations, and if there is a

few legitimate, very narrow reasons to monitor employees in this way, can it be done in a way that is in balance with the rights, the constitutional rights, with whistleblower protections, and if not, perhaps good, old-fashioned management is in order.

Mr. WALBERG. Well, should management, in speaking of that, management be responded to make sure that the law enforcement agencies are aware of their concerns, potential concerns? Is that what you would suggest?

Ms. CANTERBURY. Yes, there would be a referral to a law enforcement agency.

Mr. WALBERG. To quickly step away, refer it to a law enforcement agency.

Ms. CANTERBURY. Yes.

Mr. WALBERG. Mr. Harris, tell me about training that's being implemented since you've arrived, the directions that are going to management relative to leaks, relative to whistleblowers, how you deal with them, relative to responding to what we just discussed here about referring to an appropriate agency to deal with the law and not outside of the law.

Mr. HARRIS. So can you give me your first question again?

Mr. WALBERG. First question is, what are you doing? What training having you implemented?

Mr. HARRIS. Got it.

Mr. WALBERG. Secondly, what administrative steps have you made to make sure that the department, the agency stays out of it as much as possible, to make sure that whistleblowers understand that they're part of the agency but they're protected by the law and that there are appropriate agencies that will be brought in to make sure the law is followed?

Mr. HARRIS. Yes. There is standard training that occurs at FDA. There is when an employee comes on board an orientation, they get understanding about IT security awareness programs and trainings. There is annual training for NO FEAR, which does address the whistleblower issues. We have regular training that goes on in the information technology groups.

And so we have lots of required training every year for all of FDA to understand how security awareness works. We often, as I said earlier, the banner flashes up and makes them aware of their right to a reasonable lack of privacy. It comes up on all devices we give them.

As it relates to the management process we put in place, clearly, as I stated earlier, I would like to address Ms. Canterbury, if I could. I think this would kind of tie it all together.

Mr. WALBERG. Tie it together.

Mr. HARRIS. We consider the whistleblowers as our staff. They should not be treated any different as it relates to protection. We give everyone protection in our staff. So we don't consider them outsiders. We consider them as part of our staff.

The way we want to try to approach the issue is the committee we put together is not just myself and a couple of attorneys. There is an HR director there to determine whether we infringed on employee rights. There is IT professionals there to give Mr. Shuren in the future better information and guidance. There's a legal team. And then there is myself. When we do find that we've stepped into

an area where we have communication occurring between Congress or anybody else, again, they stop everything they're doing, nothing continues, monitoring stops, my office is notified.

Mr. WALBERG. Are you notified immediately then?

Mr. HARRIS. Immediately.

Mr. WALBERG. When they come across something, it all stops.

Mr. HARRIS. Immediately.

Mr. WALBERG. No more eyes are seeing it.

Mr. HARRIS. Nothing else happens after that. And this is why the committee is such a small group. We then bring legal into the conversation, and if it's appropriate to send it out to another law enforcement agency, we do that.

Mr. WALBERG. Well, I appreciate the answer, but I would suggest that last statement would be the approach to take more rapidly, to the outside agency.

Mr. Chairman, thank you.

Mr. FARENTHOLD. Thank you very much.

We'll now recognize my distinguished ranking member from the Subcommittee on Postal, Census, and the Workforce, the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

I want to thank all the witnesses for your willingness to testify and to help the committee with its work.

I do want to say that from an Oversight and Government Reform perspective, from this committee, our goal is to create and maintain an environment where whistleblowers can come forward. As has been said by Ms. Canterbury and the chairman and the ranking member, and Mr. Grassley earlier, our bureaucracies and these agencies and the work that they do has become so complex, whether it's financial derivatives or whether it's the FDA, some of us, it's just so complex that unless we have someone on the ground in place that comes forward, our chances of finding out about wrongdoing or misconduct is negligible.

So we really need to make sure that we have an environment there where people feel comfortable that if they have a reasonable belief that the laws are being broken, or that the public is being harmed, that they can come forward.

So there's a couple of instances. Usually the FDA flies below the radar screen. But this instance really gets me, and it's the second time recently that the FDA has just caused me to shake my head and ask what the heck is going on over there. You know, this instance it looks like there's a very robust framework in place to protect manufacturers' trade secrets. And in this case I'm not so sure anybody has ever pointed to specifically trade secrets that have been protected, but by God, we went after these employees because we thought there might be a chance that they might disclose something.

So I think it was a very, very strong response in protecting the manufacturers. I think it was very, very weak in terms of protecting the employees. And, you know, I have to acknowledge, Mr. Harris, this predates your involvement here, so I'm not criticizing you.

So I see the FDA overriding their scientists in this case. And the last time that the FDA, their conduct came to the attention of this

committee, was the approval of Zohydro, okay. Now, I know this doesn't involvement medical devices, but in that case the FDA overrode, again, their own scientific panel. Their scientists voted 11-2 that approving Zohydro, which didn't have any protections against abuse, quite similar to the early iterations of Oxycontin, so 13 scientists, 11-2, they said to the bureaucrats, do not approve Zohydro. And the FDA turned right around, right around, with an opioid epidemic in this country from coast to coast. This is one of the most serious threats to our communities, and the FDA goes ahead and puts a gun to the head of the American people by approving Zohydro. So we got this problem.

You know, personally I spend a lot of my time dealing with the effects of substance abuse in my communities. I've got three cities, major cities, and I've got 22 towns, and no one is immune. Good families, families that are struggling. It's just unbelievable. It just blows my mind that the FDA would approve Zohydro.

And so I need to put you on notice. I need to put you on notice. You have shaken my faith in the FDA because of that decision and what's going on here today. And I just want to put you on notice that, you know, I used to give people the benefit of the doubt, but I've seen such bad decisions coming out of that agency that we've got a problem, which is I've got a problem, you've got a problem. So, you know, we got to start straighten up and fly right and start doing things that are in the best interest of the American people.

And, you know, I appreciate that your mission and your goal is to do the right thing. I just think we've strayed. Sometimes the bureaucracy can do that. We just need to get back on the same page here in protecting the American people.

I've exhausted my time, Mr. Chairman. I thank you for the indulgence, and I'll yield back.

Mr. HARRIS. We will be happy to have someone provide follow-up to you on that, on this issue.

Mr. LYNCH. That would be great. Thank you, Mr. Harris.

Dr. SHUREN. And, sir, we would also be happy to talk to more details on what really was happening with these unauthorized disclosures and the impact, because, in fact, what it was doing is it was stifling other scientists. It's not that these complainants were necessarily just willy-nilly overrode. There were other scientists in the agency who disagreed with their opinion, and those people's opinion was actually being disenfranchised. People were feeling harassed, retaliated against. Other scientists were feeling retaliated against by the complainants, and they were complaining that the unauthorized disclosures was having a chilling effect on the internal discussion within the FDA and that people were afraid to put their opinions in writing because it would be disclosed to the press.

It's the same thing that Senator Grassley talked about. We want to have open discussion within the FDA. We think it is so important. But it goes on both ends.

Mr. LYNCH. Sure.

Dr. SHUREN. And we were seeing that that actually was being adversely affected, and that adversely affects public health. We cannot make well-informed decisions when that happens. And that was a misuse of those disclosures, and that's unfortunate, and they

were used to influence public meetings, and they were used to influence advisory committee meetings.

Mr. LYNCH. Well, I'll be happy to have that information offline, Dr. Shuren, and again, I thank you for your testimony.

Mr. FARENTHOLD. Thank you very much. I am going to now recognize myself for 5 minutes for a couple of questions.

First off, I want to say that whistleblowers are the lifeblood of this committee. It's dedicated government employees who see something going wrong in their agency that have no recourse other than to bring it to the attention of Congress, which is the right way to do it. It's not the right thing to do the way Mr. Snowden did it and take it to another country. And we work hard and we've passed legislation to make it safe for whistleblowers, and this committee, and I think Ranking Member Cummings will agree with me, will bend over backwards to protect a legitimate whistleblower.

In fact, the committee Web site, Oversight.House.gov, has a place you can go online to become a whistleblower. And I guess there might be a lesson in this for potential whistleblowers. Maybe the initial contact needs to be made from your home computer or a computer at the library or from a Starbucks. But you shouldn't be afraid to use your government computer to report government problems.

And, Mr. Harris, I know a lot of this happened before you got there, but you are the acting chief information officer, so I want to take a step back and maybe look at what should have been done. I mean, I understand that our computer, our rule mentality, in the private sector, you've got a lot more flexibility than you do in the public sector. The Constitution doesn't apply you due process in your private sector job. In many private sectors there are no whistleblower statutes other than potentially to the government. So as a manager you've got a lot more options in the private sector.

But in the public sector, going in and installing snooping software seems rather draconian. I would think good practice is to have something on your network that captures all incoming and outgoing mail, and then you have the ability to search that after the fact if you've got a leak. I've used EnCase before. That's a forensic software that lets you go copy somebody's computer. But, you know, nowadays with all compliance issues in various industries, there are appliances that you can put on your network that catches all the mail and saves it. And you ought to be able to search that for emails to The New York Times and have an exclusion saying if it's mail.house.gov don't show me that. I mean, it seems like it's that simple. Didn't you all hire a contractor back there? Couldn't you have told the contractor when pulling the EnCase stuff and it says mail.house.gov, I don't want to see it?

Mr. HARRIS. Yeah, I think you're on the right track. I think one thing we should note is that monitoring is actually rare. And I think what sews this together is when you think about the reasons we do monitor at times. I can give you a couple of instances. I mean, we have had cases of child pornography. In my mind, we should immediately act on that and we should immediately start to look for the issues there because the child's life is in the balance here. And then there are other instances where insider training does become an issue to protect trade secrets.

But, you know, everyone is correct. The need to protect those who whistleblow is important. So this new process that we have in place does that. It has, again on the committee, a legal individual, someone from IT, someone from HR to consider the entire range of issues that we may face before we even initiate our monitoring process.

Mr. FARENTHOLD. And it's just hard to judge what the culture of that is. You know, if within your agency there is a culture of gossip, you know, does it slip out? You've got to deal with the human elements of that as well, and I do think there needs to be a technological solution to that.

Let me go to Ms. Canterbury and get her thoughts on what the appropriate way to do this is.

Ms. CANTERBURY. So first I would like to ask why on Earth the FDA would conduct surveillance if they had suspected child pornography or insider trading occurring, why would they not go to the FBI? That just makes no sense to me. So I'm struggling with under what circumstances—

Mr. FARENTHOLD. I've run a computer consulting company. I've done this for private sector. You know, you've got an employee you think is—let's take child pornography out of it—and is just surfing porn and that's against your policy. They haven't broken the law, but they've broken your policy. So, I mean, obviously there are cases where you need to do that

Ms. CANTERBURY. Sure. And so in that case, my question would be on the back end of the review committee, I think, is a substantial structural reform, but it's only reviewing, to my knowledge, according to your interim policy, on the front end. So what would be an improvement would be to do a similar review on the back end, because there is no way you can use enough search terms to protect public whistleblowing. So if an employee is blowing the whistle with nonlegally protected information to The New York Times or to the Project on Government Oversight, that also cannot be swept up or they've been in violation of the Whistleblower Protection Act.

Mr. FARENTHOLD. And I'm going to agree with you that in many cases retrospective is the way to go.

I'm about out of time, but I will give Mr. Harris an opportunity to respond before we go to the gentelady from California.

Mr. HARRIS. Well, let me be clear. We by no stretch of the imagination are coming here today to tell you that our process is 100 percent perfect. The idea behind this is to have a methodical approach to this. And by the way, the FBI comes to us sometimes for referrals to do some of the work that we do. And so it is by no way perfect, but the only way the agency can move forward is to start something now and then we can perfect it to a point to where we can then spread it to the rest of the agency and then we all understand what our policies, rules of engagement are around monitoring.

Mr. FARENTHOLD. All right. Thank you very much. I appreciate your indulgence.

We'll now recognize the gentelady from California.

Ms. SPEIER. Mr. Chairman, thank you, and thank you to all of our witnesses.

You know, we are really very good here at calling agencies onto the carpet and beating them up and then talking to the companies in our district and hearing their complaints about the process being too slow, and the result is, is that so much innovation is going abroad because our process doesn't work.

We can't have it both ways. If we want the FDA to be more streamlined so more of this research and development of clinical trials happens here in the United States, you know, we've got to embrace that. If we don't, then we should just tell all of our constituents that if they want the new medical device that can save their lives, you're going to have to go to France or Germany to get it.

Having said that, I want to send some kudos to Dr. Shuren, because we do beat you guys up from time to time. I am sitting on an airplane 2 weeks ago coming back from going home, and the gentleman sitting next to me is a VC who specializes in medical devices, and he had nothing but praise to offer about your good work, Dr. Shuren. So I wanted you to have that at the outset.

Now, let's go to my questions. It appears that there were search terms that were developed within the administration that were superimposed on the computers of these scientists. What were those search terms? The inspector general report isn't very specific about them.

Ms. MCKEE. The search terms were "K" followed by a string of letters—

Ms. SPEIER. Right.

Ms. MCKEE. —which indicates an identification for a 510(k) submission, the word "colonography" based on the release in the article in The New York Times. And then there were also names identified of individuals where managers had voiced concerns in the management team that Dr. Shuren talked about that were performing ghost writing

Ms. SPEIER. Okay. So the first two make some sense to me. The others appear to be the beginnings of a witch hunt, and that troubles me. I think that Ms. Canterbury's concern is one that we all have in that if we want to be clear about not having reprisals it's better to have a hands-off investigation or review taking place so that it's not within the department. Go to the Justice Department, whether it's child pornography or leaks of trade secrets. And it's not your core competency anyway. So I guess the real overriding question that I have is, why not just punt these all to Justice for them to undertake the review?

Dr. Shuren.

Dr. SHUREN. Yes. So a challenge we faced back then is in the past we had our Office of Internal Affairs. That is the group who did investigations within the FDA. And due to concerns raised by Senator Grassley, and I understand those concerns, in early 2010, the policy changed. The Commissioner said in the future the Office of Internal Affairs cannot do investigations of allegations of criminal conduct for employees who made allegations against the agency. It would go to the Office of the Inspector General. But they were not doing investigations unless they had adequate evidence to do it.

And that has caught us in a bind. And in fact when just the GE letter was sent to them, they came back and said, at this time, based on the information provided, they are not taking any action, the referral lacks any evidence of criminal conduct. But after, from the monitoring, there was evidence of unauthorized disclosures. In fact, the OIG did open a formal investigation and did look into it. And at that point they decided we're not going to prosecute, but they also came back and didn't say that this wasn't wrong. In fact they said, we understand you have sufficient evidence to support administrative actions, and they closed the case at that point. In other words, this could be a problem, you are welcome to pursue it now with administrative action. And that's what happened.

Ms. SPEIER. All right. I have very little time left, but I'm concerned about the allegations by the scientists that thought that these devices were potentially unsafe or exposed people to radiation. Where are we in terms of evaluating that?

Dr. SHUREN. Yeah. So for CT colonography and their concerns about exposure radiation, it shouldn't be on the market, as I mentioned, there is a lot of evidence to support it. We think it is safe and effective. And last year there was a meeting of joint advisory committees, so two advisory committees with experts in radiology and gastroenterology, 20 people, and they unanimously felt that CT colonography should be an option for doctors and patients for screening asymptomatic individuals for colon cancer. Unanimous.

Time and time again there were issues that were brought to advisory committees, outside experts, who did not agree with the complainants. In one case, I actually set up for an issue to be brought to the advisory committee, and I let the complainants give their own individual perspective. Actually had two perspectives. We never do that. We have the center provide a unit, one perspective, and here I said there is difference of opinion, I want to put sunshine on it, didn't hide from it, put sunshine on it and get feedback, and the advisory committee didn't agree with the complainants.

And scientists within the agency, there were many scientists who didn't agree. And many of our managers, they are scientists. These people are also experts. And they disagree, and that's okay. People can disagree. They should disagree if they feel that way, and we have a process if they disagree, how they can appeal that.

Unfortunately, never took advantage of that process, which actually brings it all the way up to my office, can even bring it up to the Commissioner's office, and it has to be in writing and they have to justify their rationale, and never took advantage. Instead, it was put information that by law is prohibited to be disclosed by any FDA employee, whistleblower or not, and put that out in the public venue. And that does adversely affect public health, it adversely affected discussion within the agency, and it adversely affected the very issue of open dialogue, which they were complaining about. In fact, in one investigation, independent investigation, it was found that it was one of the complainants who was creating the hostile work environment.

Ms. SPEIER. I thank you. My time has expired.

Mr. BENTIVOLIO. [Presiding.] Thank you.

At this point I'll recognize myself. I would like to thank each of our panelists for being here today.

Mr. CUMMINGS. Yeah, I just want to close.

Mr. BENTIVOLIO. Okay. Well, I'm going to ask a few questions.

Mr. CUMMINGS. Oh, okay. Sure.

Mr. BENTIVOLIO. Briefly.

But, Doctor, you've answered a few of my questions. But after listening to testimony and the questions that were asked, I seem to have all my questions answered. But there seems to be an underlying problem that you just addressed, is that, you know, when you have a whistleblower there is procedures to follow to make your points, to make your complaint heard, correct? And you've just explained that procedure. But there is, according to your testimony, if I understood this correctly, they didn't follow all the procedures and went over and above and then contacted Congress or blew the whistle, so to speak.

Dr. SHUREN. No. They are welcome to contact Congress. The issue was they disclosed confidential information that is prohibited by law from disclosure to members of the public, including the press.

It was never about Congress. None of this had anything to do about Congress. They had been complaining to Congress for 18 months before this started.

When I first started at the Center was in September 2009. Before I could even speak to any of my staff and hold an all-hands, my first two days, I spent a lot of it on Capitol Hill, at the request of congressional staff, to talk about them and their complaints. They were complaining all the time, which is fine. No one objected. And I kept hearing they were constantly complaining.

If anyone was going to retaliate, they would have done that well before. This was in response to unauthorized disclosures. And the OIG even concluded that there was reasonable concern for doing the monitoring.

Now, people will have issues about how that was done, but that is a different issue. This was nothing to do with retaliation. There was no targeting of Congress. The OIG concluded that was well. There was no targeted of protected disclosures by whistleblowers. None of that.

Mr. BENTIVOLIO. Thank you, Doctor.

Ms. Canterbury.

Ms. CANTERBURY. So, the Inspector General did not confirm that there were disclosures of unauthorized information.

The staff report, the Issa-Grassley report, explicitly says that they did not find evidence of unauthorized disclosures in their surveillance of the employees, of the whistleblowers.

And I wanted to go back to one other thing that Dr. Shuren said about the IG refusing to conduct an investigation for lack of evidence.

The IG declined on May 18th in 2010 to investigate for lack of evidence of criminal activity, but also pointed out to the agency at that time that 5, U.S.C., section 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—to the media and Congress—as long as the material released is not specifically prohibited by law or protected by executive order and classification.

So that is what they got back, was their first determination, their first warning, not to violate whistleblower protections.

When they went back to the IG and asked for a review, the IG looked at whether or not these unauthorized disclosures were in violation of the law, consulted with the Department of Justice, and, in fact, found that no further action would be taken.

DOJ declined to prosecute. The OIG declined to investigate it further. There was no evidence of prohibitions of law.

What the IG said in the letter was not that there was sufficient information to take administrative action, but, instead, it said your office indicated it had developed sufficient evidence to address the misconduct through administrative process.

So the message from the IG was not that we think you have sufficient evidence, but you say you do; so, go ahead and take care of it administratively.

Dr. SHUREN. Yes. But the OIG in the first place was actually making clear you can have certain disclosures to the media unless it is prohibited by law. That was the whole point.

The kinds of disclosures that were occurring, and the ones we were concerned about—

Mr. BENTIVOLIO. Doctor, I think what really concerns me is that, when an employee, a scientist, raises a red flag on some medical equipment or medical product and they bring it to the attention of the people in charge of the agency and, yet, for some reason, their issues aren't addressed to their satisfaction, they have to go outside of the agency to get redress.

I think—to me, you know, after listening to all this testimony, it seems to be a cultural problem within a lot of government agencies, not just the FDA. So I think that is the thing we really need to focus on.

Why can't an employee, a scientist, probably one of the smartest people in that agency, have some concerns and those concerns be addressed in-house and taken care of? And, yet, even if you have to put in some overtime.

Dr. SHUREN. I would agree with you. And actually—

Mr. BENTIVOLIO. But, apparently, those aren't there. You have not created a culture—or the FDA has not created a culture where those things can be addressed and the public can be satisfied. And I think I am out of time.

And now Mr. Cummings.

Mr. CUMMINGS. Thank you.

Thank you very much, Mr. Chairman.

Looking at the report of the IG, Mr. Harris and Mr. Shuren, it says—and it is on page 20 of the report—it says, “Given this, FDA’s interim policy addresses our five recommendations outlined above. HHS should determine whether all other individuals OpDiv policies meet our recommendations above. HHS also should regularly review and, as necessary, update its Department-wide monitoring policies to ensure they are compatible with new and emerging technologies and methodologies. Information technology is continually changing, and a static monitoring policy could fail to address key implementation issues as capabilities evolve.”

And I just want to make sure—it sounds like the IG is satisfied for the moment. But as he says, the technology is continuously

changing. And as you know, you can have technology today that is outdated today.

And so the question becomes, you know—I want to—what I am going to do, Mr. Chairman, with Chairman Issa, is try to follow up with the IG to make sure that he is satisfied that everything that can be done at this moment, consistent with his recommendations, has been done.

And, number two, I am just curious as to how you plan to keep up with the technology and make the changes that are necessary so that we are not outdated.

Mr. HARRIS. Thank you, sir.

Clearly, as we stated earlier, we don't consider this process as anywhere near completed. Instead of static, it has to be fluid. We have to keep up with the emerging technologies. I mean, there is a smart kid somewhere who is able to come up with an idea of how to breach our system. So we have to always be out in front of the process.

But going back to the earlier statement that we know that we need to have a set of clearly understood processes across FDA that requires us to have, again, approval before anything starts, I think the IG is also stating that we started out pretty good, but we still have much more work to do. We recognize that. The agency recognizes it. So we are in no way saying that we are done here. We have a lot of work to do.

Mr. CUMMINGS. I know the chairman was about to end the hearing; so, I will just finish my closing right here. I know. I saw him. That is why I said "was about to."

I just want to thank all of you for being here.

And I want to reiterate the comments of Congresswoman Speier and, also, Lynch. It is so important that government operates correctly because, when government does not operate correctly, there are consequences.

I go to the same bank every Friday. For the last five months, I have been following my teller, whose son's wife was having—well, his girlfriend was having twins. And so, you know, everybody's excited and everything.

And then about a week ago I went in and I said, "Well"—you know, she was so excited that these twins were going to be born. And they knew it was two boys.

I was excited for her, and I would ask about them every time I walked in the bank. And then she said, "They have been born" and then she said, "I have got good news and bad news." She said, "The boys are fine. The mother's in a coma." Apparently, there was some complications. Developed MRSA in the hospital. And then, when I came back last Friday, she said she died.

Whether this was with regard to a device, I don't know. I am not saying it is. But now we have got two boys a week old who will go for the rest of their life without their mother. Those are the consequences.

I think a lot of times we here in government forget that there are people that are affected by our decisions, but they are. And so I think—first of all, I don't think, to be frank with you, that a whistleblower has a right to remain silent if they see something wrong. That is why we want to protect them. We want to get it right.

I am asking you all, when you go back to your shops, to reiterate that. We are going to continue to follow this. I know the chairman will and our committee will. But this is so very, very, very important.

And I heard you, Ms. Canterbury, and, basically, what you were saying was, "Look, we don't trust that this is going to work out. It is not all complete" and all that.

Well, it has got to work out. It has to work out because the American people deserve absolutely nothing less. That is why they pay our servants—our Federal servants, employees, to do these jobs.

And going back to something Chairman Issa said, it is also about trust. So the more we do it right, like you said, Mr. Shuren, when you were talking about dismissing everybody or however—you know, when you said you were trying to make sure that the whistleblowers were protected, those are the kinds of things we have to continue to do because the public needs to feel that trust, and we have got to make sure that we take care of them.

So I want to thank you very much.

I am out of time, Ms. Canterbury, but that is up to the chairman.

Ms. CANTERBURY. I just want to say that I have full trust that, if you and the chairman work together, that you will get the job done right.

Mr. CUMMINGS. Thank you very much. And we will. Thank you.

Mr. BENTIVOLIO. At this time I would like to recognize the gentleman from Florida, Mr. Mica.

Mr. MICA. Well, thank you, Mr. Chairman, and ranking member.

I came in a little bit late. I will try to ask a couple of questions, hopefully, that haven't been asked.

I was going to turn my first question to Mr. Harris. Mr. Harris, in September, I guess, of last year, you were acting CIO and you released an interim policy staff manual and guide for employees' computer monitoring.

You have both the role, I guess, of—is it COO and, also, CIO?

Mr. HARRIS. Yes, sir.

Mr. MICA. Okay. Now, in that capacity and in developing that manual, under the interim policies, what are your responsibilities as both the COO and, also, as the chief information officer?

Mr. HARRIS. As the COO, it is my responsibility to make sure that the process is fluid and that it is commonly understood by all.

As the chief information officer, it is to make sure that we give good guidance to program officers and centers across FDA when they have a request to look at issues that may occur within their centers.

And so there is two separate hats there. One is of processes. I mean, this is not about power. This is really about well-matured processes that the entire agency can understand what we are doing from A to Z.

And from an IT perspective—Dr. Shuren spoke of it earlier—the question was asked whether we could have taken a different approach.

I think, as an IT professional, I would have said that we need to look at the entire scenario so we can determine the most appropriate approach.

Mr. MICA. Well, do you think, again, with you in the position of being both COO and CIO, there is a potential conflict?

Some of your responsibilities are for the approval of the monitoring, the execution of the monitoring, and the direction, but, also, the review of the monitoring.

Do you see that as something that actually should be kept separated? I don't know how you are able to achieve your sort of—I would see it as in competing roles. What is your opinion?

Mr. HARRIS. Well, the review committee that we have as part of our steps does have legal review included in it. So when it comes to—as a formal request, there is a committee, again, that has an HR person on it, has an IT person, a legal person on it. And then it comes back to me.

So they have an opportunity to look at it without me even being present. But I think the most important part of this is the legal review takes place and then, before anything starts—

Mr. MICA. So you are saying on top of this there is another review that would ensure, again, some objective review?

Mr. HARRIS. Yes.

Mr. MICA. Ms. Canterbury is answering—or shaking her head “no.” Did you want to respond?

Ms. CANTERBURY. I understand from the interim policy that there is a legal review on whether or not to conduct the surveillance.

But once the information is collected, it is Mr. Harris who maintains that and determines who gets to use that information and how it is used.

And so my recommendation is that the COO shouldn't be involved. As you suggest, sir, I think it may be a conflict of interest.

He should not have a part in all decision-making and then control what—the information that is collected at the back end.

Certainly, at the back end, there has to be a legal review to make sure—

Mr. MICA. So you don't think that even though what he cited and considers as another step is not really doing the job because, again, just the nature of the conflict of his having both of those responsibilities—I mean, I don't want to put words in your mouth. Is that correct?

Ms. CANTERBURY. Right. My concern is with, after the information is collected, what happens to it.

Mr. MICA. Right.

Ms. CANTERBURY. Are there protected disclosures swept up in what is collected? And only Mr. Harris would get to decide that, according to the interim policy.

Mr. HARRIS. I think, again, we stated earlier that the policy is nowhere near complete. We made a conscientious choice to have an interim policy so that we can get this right, and this has to be done right over time.

There are many scenarios that apply here that don't have a single answer to it.

The other piece of it is that we want the agency to begin to move forward and, one, again, protect the whistleblowers, and, two, make sure that our processes are commonly understood from end to end.

And then, at the end of the day, before anything begins, anything begins, we have to have an approval.

And so I don't know what happened, again, 2 or 3 years ago, but I know now that we have a much more well-oiled process.

It is interim. It is not perfect. We have to build it as we go because, as Mr. Cummings said earlier, the landscape changes with IT on a regular basis. We have to be fluid with it if we are going to stay on top of things.

Mr. MICA. Also, again, in protections and making certain that important responsibilities are fulfilled. I think Ms. Canterbury did allude to, again, some conflict that exists just by the nature of the current way this is conducted.

Mr. HARRIS. That is right. It comes out of my hands and goes, as we talked about, to the legal review. We call it a legal tank team. When something has occurred that needs to have a set of fresh eyes on it, it comes out of my hands and goes into the hands of a legal team, who looks at it, and we call them a tank team. They then decide the best recourse of action from there.

So I think it would probably be better if we could at some point in time have some conversations about what we are doing because, I think, again, from where we were 2 or 3 years ago, night and day.

Mr. MICA. Well, again, we wouldn't be holding this hearing if it all worked right. But that is why we are here.

Let me turn—a final question just to Ms. McKee. You are involved in, again, some of the monitoring. Is that correct?

Ms. MCKEE. That is correct.

Mr. MICA. Yeah.

And did anyone ever tell you that it was inappropriate to look at disclosures to OSC or members of Congress or attorneys? Did they tell you that?

Ms. MCKEE. The focus of the monitoring wasn't on any of those disclosures. While they may have been captured broadly, it was not something that we looked at.

Mr. MICA. Okay. And did you think that it was fair game, because they were doing it on an FDA computer, that they could again look at that information and make the disclosures?

Ms. MCKEE. I am sorry. I don't understand your question. They could look at it?

Mr. MICA. Again, you thought it was fair game because they were using an FDA computer in the process.

Ms. MCKEE. The software that was used captures everything, is my understanding. There was not a way to wall off different communications—types of communications.

Mr. MICA. Well, again, you—but you thought it was appropriate use of computers and information?

Ms. MCKEE. I am not getting your question. I am sorry.

Mr. MICA. Again, you said to the committee that you were involved in this process.

Ms. MCKEE. That is correct.

Mr. MICA. And you, in fact, had said that it was inappropriate to look at disclosures—or you said there was not a problem with looking at disclosures to either OSC or members of Congress or attorneys, is what I—some of the information I have been provided. That is not correct?

Ms. MCKEE. I don't believe that is correct, sir. It may have been a mistake, misspoke during an interview.

Mr. MICA. Well, again, I am looking at information that was provided from your transcribed interview. And, furthermore, when questioned about this, I am informed that you thought it was fair game because they were doing it on an FDA computer. And I think you responded—at least in those interviews, you thought it was a fair game because, again, they were using FDA computers.

Ms. MCKEE. If I recall—I am trying to put your question into context with the question I was asked—I believe monitoring FDA employees' computers is fair game.

Mr. MICA. Is fair game under the rules. And you still believe that.

Ms. MCKEE. I believe there are times when it is appropriate, yes, to monitor FDA employees' computers.

Mr. MICA. Okay. And about—what about disclosure of that information? What is your feeling about what has taken place and how that has worked?

There have been disclosures from the monitoring that are inappropriate. And, obviously, the monitoring, again, monitors people's inappropriate activity. That is part of the purpose of the monitoring. Correct?

Ms. MCKEE. That is correct.

Mr. MICA. Okay. And what is your opinion as to how this has worked and functioned? You said it is fair game, which they are doing. They are conducting this monitoring. And, obviously, we have had problems with it not working. What is your opinion? What is the flaw? Where do we need to go?

Ms. MCKEE. I certainly believe the processes that the agency has put in place in the last six months would have helped in the situation—

Mr. MICA. If it had been in place.

Ms. MCKEE. If it had been in place in 2010, it certainly would have helped.

Mr. MICA. Okay. Thank you.

Yield back.

Mr. BENTIVOLIO. Thank you.

At this time I would like to thank all of our witnesses for taking time from their busy schedules to appear before us today.

The committee stands adjourned. Thank you very much.

[Whereupon, at 12:27 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**REVIEW OF THE FOOD AND DRUG
ADMINISTRATION'S COMPUTER
MONITORING OF CERTAIN
EMPLOYEES IN ITS
CENTER FOR DEVICES AND
RADIOLOGICAL HEALTH**



**Daniel R. Levinson
Inspector General**

**February 2014
OIG-12-14-01**

Office of Inspector General

<http://oig.hhs.gov>

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Table of Contents

EXECUTIVE SUMMARY	2
REVIEW OF THE FOOD AND DRUG ADMINISTRATION'S COMPUTER MONITORING OF CERTAIN EMPLOYEES IN ITS CENTER FOR DEVICES AND RADIOLOGICAL HEALTH.....	5
I. FDA'S COMPUTER MONITORING	5
Events Prior to Computer Monitoring	6
The Decision To Monitor Scientist 1.....	8
Monitoring Software Used by FDA.....	10
Computer Monitoring of Scientist 1 Begins	11
The Interim Report of Investigation	12
Computer Monitoring of Additional Scientists Begins	13
Procedures Used During FDA's Computer Monitoring	14
FDA Consultations With OGC	15
CDRH Takes Action as a Result of Monitoring.....	15
II. FINDINGS	16
III. RECOMMENDATIONS	18
IV. DEPARTMENT RESPONSE	20
APPENDIX A: Methodology.....	21
APPENDIX B: CDRH and the Premarket Application Process	22
APPENDIX C: Applicable Legal Criteria.....	23
Reasonableness of a Computer Search	23
Interception of Electronic Communications	24
The Whistleblower Protection Act.....	25
Prohibitions on the Disclosure of Information by FDA Employees.....	25
Appendix D: Department Comments.....	27

EXECUTIVE SUMMARY

On July 14, 2012, *The New York Times* reported on computer monitoring by the Food and Drug Administration (FDA) of certain scientists in FDA's Center for Devices and Radiological Health (CDRH). On July 20, 2012, the Secretary of the U.S. Department of Health and Human Services (HHS) wrote to HHS's Office of Inspector General (OIG), asking it to consider whether there was a sufficient basis to conduct the monitoring; to consider whether the methods of monitoring were appropriate; and to provide recommendations on how HHS can appropriately, effectively, and efficiently investigate allegations of improper dissemination of confidential information while protecting employees' rights and whistleblower protections.

Between April 2010 and October 2011, the FDA used computer-monitoring software on the FDA computers of five CDRH scientists. FDA suspected that these employees were sending trade secrets or confidential commercial information (CCI) outside FDA in possible violation of FDA regulations and criminal statutes; FDA also was aware that these employees may have held whistleblower status. During the time immediately prior to and during the computer monitoring, FDA computer systems displayed a log-on banner that stated that users had no right of privacy in the system and that all data on the system may be monitored; however, FDA had no policy governing the approval or conduct of such monitoring.

During 2009 and 2010, several newspaper articles referenced or quoted internal CDRH memorandums. One such article, published in *The New York Times* on March 28, 2010, referenced a confidential GE Healthcare submission to CDRH and quoted CDRH employee Scientist 1.¹ Soon after, FDA received a complaint letter from counsel representing GE Healthcare that alleged that its CCI had been disclosed to the press by CDRH in violation of Federal regulations and agency policy and asked FDA to investigate. CDRH management strongly suspected that Scientist 1 was the source of the information in the article because, among other reasons, he was quoted in the article. CDRH management also suspected that Scientist 1 was inappropriately ghostwriting reports for his subordinates.

CDRH's Director tasked CDRH's Executive Officer with finding out what options were available to identify the source of the disclosure to *The New York Times* and to prevent future unauthorized disclosures. In order to accomplish this, the CDRH Director instructed the CDRH Executive Officer to engage with FDA's Assistant Commissioner for Management and/or with FDA's Chief Information Officer (CIO). After the CDRH Executive Officer met with both the

¹ OIG has redacted the names of the five scientists subject to computer monitoring since they may have been entitled to protections under the Whistleblower Protection Act, even though their names already are known to the Department. In an abundance of caution and in an effort to avoid the appearance of disclosing the names of whistleblowers, we refer to them as Scientists 1 through 5.

Assistant Commissioner for Management and the CIO, the CIO, in conjunction with the Chief Information Security Officer (CISO), proposed investigating the leaks using computer-monitoring technology. Office of Information Management (OIM) staff arranged to begin monitoring Scientist 1's computer and chose the monitoring tools that were used.

OIM staff chose two computer monitoring tools to investigate Scientist 1. They used EnCase to image (or copy) the memory of Scientist 1's FDA computer, which, at times, included personally owned removable memory drives connected to the FDA network. OIM staff also chose SpectorSoft (Spector) and installed it on Scientist 1's computer. Spector captures: (1) screen shots of a user's computer every few seconds and (2) the user's keystrokes, including keystrokes used to enter passwords.

Using a short list of search terms developed by CDRH's Executive Officer, OIM staff reviewed the screen shots taken of Scientist 1's computer for potential indications of unauthorized disclosures outside FDA or ghostwriting. Because Spector takes screen shots of the information displaying on a user's computer every few seconds, OIM staff could not scope Spector to capture only information relevant to the issues CDRH wanted investigated; rather, OIM staff manually reviewed the tens of thousands of screenshots after they were taken by Spector to cull out those that appeared relevant to certain search terms concerning unauthorized disclosures and ghostwriting. Accordingly, while we found no evidence that FDA used Spector to target specifically the scientists' communications with any particular person or group, such as Members of Congress or the media, it is precisely because Spector broadly captured information that the scientists' communications with such persons were captured.

Partly on the basis of information discovered while monitoring Scientist 1's computer, CDRH management directed OIM staff to expand Spector and EnCase monitoring to include four additional CDRH scientists. We found no evidence that during the computer monitoring, OIM staff logged into any FDA user's computer in order to gain live access as a user of the computer or attempt to log into any FDA user's personal Web-based email accounts. While Spector captures by default the user's keystrokes—including keystrokes used to enter passwords—we found no evidence that anyone at FDA, CDRH, or OIM ever accessed Spector's keystroke logs, where such information resides.

As a result of the computer monitoring, CDRH concluded it had developed evidence that certain employees had disclosed CCI. In the spring of 2011, CDRH wrote to several companies that had submitted confidential materials to CDRH to inform them that it had determined that an employee had made, via email, unauthorized disclosures of their CCI in July or August 2010.

On the basis of its review, OIG found that despite the reasonableness of CDRH's concerns and the explicit language in FDA's network log-on banner, CDRH failed to fully assess beforehand, and with the timely assistance of legal counsel, whether the scope of potentially

intrusive EnCase and Spector monitoring would be consistent with constitutional and statutory limitations on Government searches and consistent with whistleblower protections. OIG recommends that HHS ensure that its operating divisions draft and implement policies and related procedural internal controls that provide reasonable assurance of compliance with laws and regulations, particularly those governing current and prospective employee monitoring. In September 2013, FDA issued an interim computer-monitoring policy that addresses our recommendations.

REVIEW OF THE FOOD AND DRUG ADMINISTRATION'S COMPUTER MONITORING OF CERTAIN EMPLOYEES IN ITS CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

This review responds to the Secretary's letter dated July 20, 2012, asking the Office of Inspector General (OIG) to review the monitoring of electronic communications of certain employees in the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH). Specifically, the Secretary asked OIG to consider whether there was a sufficient basis to conduct the monitoring; to consider whether the methods of monitoring were appropriate; and to provide recommendations on how the U.S. Department of Health and Human Services (HHS) can appropriately, effectively, and efficiently investigate allegations of improper dissemination of confidential information while protecting employees' rights and whistleblower protections.

The Secretary's request refers to the computer monitoring of five individuals at CDRH that began on April 22, 2010, when FDA installed SpectorSoft monitoring software (Spector) on the Government-issued computer of Scientist 1. FDA subsequently expanded its monitoring to the Government-issued computers of Scientist 2, Scientist 3, Scientist 4, and Scientist 5. FDA also used a product called EnCase to remotely take forensic data images of the individuals' computer and network memory. Although FDA monitored each individual's computer usage for varying lengths of time, FDA had ended its monitoring of all five individuals by October 9, 2011.

This review is organized into four sections. Section I summarizes events that led to the computer monitoring and FDA's conduct of the monitoring, Section II presents OIG's findings, and Section III provides OIG's recommendations. Section IV presents the Department's response. Appendixes cover OIG's methodology, CDRH and the premarket application (PMA) process for medical devices, the legal criteria relevant to the disclosure of information by Federal employees and computer monitoring of Federal employees, and the Department's comments.

I. FDA'S COMPUTER MONITORING

This narrative of the facts and events leading to FDA's computer monitoring, the deliberation and authorization by FDA management relating to the computer monitoring, and FDA's conduct of the monitoring is the result of the interviews and the document review described in Appendix A. Our review uncovered few inconsistencies among the information provided by interviewees and obtained from documentation, but where there was ambiguity or conflict, we note it.

During the time immediately prior to and during the computer monitoring, FDA used a network log-on banner, which appeared each time an employee logged onto his or her computer, prompting the employee to press “OK” to continue.² It read:

This is a Food and Drug Administration (FDA) computer system and is provided for the processing of official U.S. Government information only. All data contained on this computer system is owned by the FDA and may, for the purpose of protecting the rights and property of the FDA, be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed by and to authorized personnel. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISCLOSURE. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Authorized personnel may give to law enforcement officials any potential evidence of crime found on FDA computer systems. Unauthorized access or use of this computer system and software may subject violators to criminal, civil, and/or administrative action. The standards of ethical conduct for employees of the Executive Branch (5 C.F.R. § 2635.704) do not permit the use of government property, including computers, for other than authorized purposes.

Events Prior to Computer Monitoring

On January 13, 2009, *The New York Times* published an article that included potentially confidential information from a then-pending 510(k) submission³ for a mammography computer-aided detection device from device manufacturer iCAD.⁴ CDRH officials stated that these disclosures were not authorized. Therefore, the disclosures would have been in violation of FDA regulations.⁵ According to information iCAD provided to FDA by letter dated that same day (the iCAD Letter), the article’s author informed the company that he had received “internal FDA documents” regarding the device from “scientific officers of the FDA.” The iCAD Letter enclosed copies of two January 8, 2009, news articles by the Associated Press and *The Wall Street Journal* that reported on a letter sent by a group of FDA scientists to then President-Elect Barack Obama’s transition team complaining that the scientific review process for medical devices at FDA had been corrupted and distorted by FDA managers and singling out

² FDA since has updated the language in its log-on banner to meet OIG recommendations.

³ CDRH’s PMA process, and the 510(k) process in particular, are described in Appendix B.

⁴ Gardiner Harris, *In F.D.A. Files, Claims of Rush to Approve Devices*, *The New York Times* (Jan. 13, 2009).

⁵ Several statutory and regulatory provisions limit the ability of FDA employees to share agency information with others outside the agency and are discussed in detail in Appendix C. They include 18 U.S.C. § 1905 (Federal criminal statute generally limiting disclosures), 21 U.S.C. §§ 331(j) and 333 (additional criminal provisions in the Federal Food, Drug, and Cosmetic Act that prohibit disclosure of trade secrets (but not confidential business information) submitted to FDA in accordance with FDA approval processes), and 21 CFR § 814.9 (FDA disclosure restrictions with respect to PMAs).

mammography computer-aided detection devices as an example of a technology that should not have gone forward. The iCAD Letter pointed out that *The New York Times*, and possibly other media outlets, had obtained material relating to 510(k) submissions on mammography computer-aided detection devices. *The New York Times* article quoted from an internal agency memorandum regarding the pending review of another firm's premarket 510(k) submission. The quoted memorandum was a consultation review memorandum on the 510(k) submission that had been drafted on March 14, 2008 (and updated on March 26, 2008), by CDRH personnel and addressed to, among others, Scientist 1.

On October 1, 2009, the Acting Director of CDRH and other CDRH staff participated in a telephone interview with *Wall Street Journal* reporter Alicia Mundy, who had co-authored the January 8, 2009, article enclosed with the iCAD letter. During the call, Ms. Mundy quoted an internal FDA 510(k) reviewer memorandum that contained what CDRH believed to be CCI, the disclosure of which is restricted by regulation, or potential trade secrets, the unauthorized disclosure of which may have constituted violations of criminal statutes.⁶ The CDRH Freedom of Information Act (FOIA) officer later confirmed that this particular reviewer memorandum had not been requested or released under FOIA.

On October 1, 2009, CDRH requested an audit of its internal electronic imaging system, IMAGE, to determine which employees had accessed the files containing the disclosed materials. The audit identified Scientist 1 as the only person who had accessed the particular files without a valid reason.

On March 28, 2010, *The New York Times* published another article on FDA's 510(k) process, which described allegations that FDA downplayed the risks of radiation exposure when considering applications for the approval of certain uses of radiological devices. The article stated that "a group of agency scientists who are concerned about the risks of CT scans say they will testify at [an FDA meeting on how to protect patients from unnecessary radiation exposure] that FDA managers ignored or suppressed their concerns..." The article reported that General Electric (GE) had submitted a 510(k) application and referenced "[s]cores of internal agency documents made available to the New York Times" pertaining to it.⁷ The article quoted comments made in internal FDA communications by Scientist 1 (see note 1 on page 3) and a former CDRH contractor in opposition to the GE submission. The article also mentioned internal discussions from a May 12, 2009, 510(k) premarket review meeting that CDRH believed to be privileged.

⁶ *Ibid.*

⁷ Gardiner Harris, *Scientists Say F.D.A. Ignored Radiation Warnings*, *The New York Times* (Mar. 28, 2010).

On April 16, 2010, FDA received another complaint letter, this time from counsel representing GE Healthcare (the GE Letter). The GE Letter expressed disappointment in CDRH for disclosing to the press CCI contained in a 510(k) submission for a GE Healthcare device used in CT (computed tomography) colonography screening. The GE Letter asserted that “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.” The GE Letter requested that FDA conduct an investigation of the leak.

The Decision To Monitor Scientist 1

According to the CDRH Executive Officer, Scientist 1 was selected for computer monitoring in part because he was named in the March 28, 2010, *New York Times* article, which was referenced by and enclosed with the GE Letter. (The other FDA scientist named in the article was no longer an employee of CDRH at the time the GE Letter was received.) In addition, the audit requested by CDRH on October 1, 2009, of FDA’s internal IMAGE System had identified Scientist 1 as the only person who had accessed the particular files without a valid reason.

On April 21, 2010, CDRH’s Executive Secretariat brought the GE Letter to the attention of CDRH’s Executive Officer, who shared a copy with the CDRH Director. The CDRH Director directed CDRH’s Executive Officer to find what options were available to identify the source of the unauthorized disclosure and to prevent future disclosures. The CDRH Director also told her to share the GE Letter with FDA’s Chief Information Officer (CIO) in FDA’s Office of Information Management (OIM) and FDA’s Assistant Commissioner for Management.⁸ The CDRH Director instructed the CDRH Executive Officer to meet with the Assistant Commissioner for Management and/or the CIO to discuss the unauthorized disclosures. The CIO, in conjunction with the Chief Information Security Officer (CISO) and others, arranged to begin monitoring Scientist 1’s computer. The CDRH Director was told about this monitoring at the time and approved it. It does not appear that any other response, apart from computer monitoring, was considered.

The CISO and the CDRH Executive Officer met with the Team Leader for Incident Response at Chickasaw Nation Industries, Inc. (CNI), (the CNI Team Leader), an information security contractor for FDA, to explain CDRH’s concern that Scientist 1 was disseminating information outside the FDA network. According to the CNI Team Leader, CDRH also was

⁸ Additional FDA officials, including the Chief Counsel of FDA and the Special Agent in Charge (SAC) of FDA’s Office of Internal Affairs also received copies of the GE Letter.

concerned that Scientist 1 was improperly preparing official CDRH reports in the names of other CDRH scientists (or ghostwriting them), on the basis of complaints from the other scientists' supervisors. The group discussed how to implement the CIO's monitoring directive to investigate these allegations.

At the time, neither HHS, FDA, nor CDRH had implemented a policy governing the computer monitoring of employees designed to ensure compliance with limits on Government searches of Government employees, such as the Fourth Amendment, the prohibition on intercepting electronic communications (Title III of the Omnibus Crime Control and Safe Streets Act (Title III)), and the protections in the Whistleblower Protection Act (WPA).⁹ The only guidance issued by FDA that governed computer monitoring was FDA's *Forensic & Incident Response Procedures Manual*, which is a technical document based on technical guidance from the Department of Commerce's National Institute of Standards and Technology. It does not provide guidance to managers on how to conduct investigations, office searches, or computer monitoring.

During the meeting, the CDRH Executive Officer gave the CNI Team Leader a piece of paper listing search terms she had developed. This page of notes established the parameters for the initial computer monitoring of Scientist 1. The page read:

Search terms:

Colonography

*K followed by a string of numbers*¹⁰

It is possible that the employee had "ghost written" for the following employees:

[Scientist 3]

[Scientist 2]

[Scientist 4]

[Name Redacted]

[Name Redacted]

[Scientist 5]

⁹ As described more fully in Appendix C: (1) the Fourth Amendment requires that Government searches of Government employees be justified in their inception and permissible in scope; (2) Title III establishes criminal penalties for the interception of electronic communications absent an applicable exception; and (3) the WPA prohibits retaliation against a Government employee for disclosure of evidence of violations of law or regulation, waste and abuse, or a specific danger to the public health. Other statutes, such as the Privacy Act, may also impose limits on such monitoring.

¹⁰ "K followed by a string of numbers" refers to Premarket Notification filings in accordance with section 510(k) of the Federal Food, Drug and Cosmetic Act, in which such filings are labeled with "K" followed by a series of digits.

The list of employees identified as possible recipients of Scientist 1's ghostwritten material was based on complaints by their supervisors that work they were turning in was not their own.

Monitoring Software Used by FDA

Around the same time, the CISO met with the CNI Team Leader to discuss available software tools that could be used to carry out the computer monitoring. FDA ultimately chose two tools to monitor computer usage of the scientists: SpectorSoft (Spector) and EnCase. Spector monitors a user's ongoing computer activity by capturing screen shots at a set interval (for example, every 5 or 10 seconds) and recording keystroke data. Spector cannot be used to see a user's activity in real time; rather, it displays static screen shots that it has captured. The CNI Team Leader believed Spector was the best tool to use in this situation because it was responsive to concerns of ongoing data exfiltration. The CNI Team Leader stated it is generally impossible to find evidence of transmissions of data beyond the FDA network that occurred in the past because individuals typically use personal Web-based email to communicate and transmit such data.¹¹ He also stated that OIM could remotely install Spector on a computer that is part of the FDA network without the individual's knowledge and that Spector would transmit its data to the Incident Response team.

Spector captures by default the user's keystrokes—including, but not limited to, keystrokes for passwords. The member of CNI's Incident Response Team (the CNI Team Member) ultimately assigned the computer-monitoring project stated that no one else at CNI ever looked at the keystrokes. Furthermore, he knew that no one at FDA looked at the keystrokes either, because only he was in a position to provide access to the keystroke logs and he never received such a request. The CNI Team Member told OIG that during the monitoring, CNI staff never logged into an FDA user's asset to gain live access as a user of the asset, nor did the CNI Team Member attempt to log into any FDA user's personal Web-based email accounts. Similarly, the CNI Team Leader told OIG that during the computer monitoring, he and his team members never physically or remotely controlled anyone else's computer.

Screen shots that CNI identified as showing potential indications of ghostwriting or unauthorized disclosures outside FDA were shared with CDRH for further review. CDRH's then Associate Director, Office of In Vitro Diagnostic Device Evaluation and Safety, was given primary responsibility for reviewing these selected screen shots to look for CCI or trade secrets

¹¹ OIM staff told OIG that no tool available to FDA at the time could re-create communications over earlier non-FDA Web-based email because Web-based e-mail leaves very few traces behind on a user's computer.

being sent outside FDA, because she had subject matter expertise on the medical devices that CRDH reviews.

EnCase is a retrospective tool that can remotely create a forensic data image of a hard drive or other computing asset. EnCase was not able to easily show whether data that existed on an FDA asset had been transmitted beyond the network. However, FDA used EnCase to take an image of the scientists' computers and network memory several times, usually in an attempt to recover something seen on a Spector screen shot relevant to unauthorized disclosures or ghostwriting, such as an email attachment that appeared likely to contain CCI. When CDRH requested a document, such as an e-mail attachment, CNI staff used EnCase to recover the file and then transferred the attachment and any other files to CDRH via an encrypted FDA USB storage device.

Computer Monitoring of Scientist 1 Begins

On April 22, 2010, the CNI Team Leader remotely installed Spector on Scientist 1's Government-issued laptop. The CNI Team Leader subsequently assigned the project to a subordinate, the CNI Team Member, giving him a page of "specifications" he had drafted together with the page of search terms drafted by the CDRH Executive Officer. The CNI Team Member described them as a text file containing "directions and guidance for the FDA task," but FDA did not provide a copy of the specifications to OIG.

On April 23, 2010, FDA's Assistant Commissioner for Management informed FDA's Office of Criminal Investigations (OCI) about the GE Letter allegations, and OCI advised that it believed the issue should be referred to OIG because the individual alleged to have made the disclosure was also involved in a series of ongoing whistleblower/Qui Tam issues with CDRH.

OCI opened a case regarding the allegations in the GE Letter on May 14, 2010, and, by letter dated the same day, wrote OIG's then-Assistant Special Agent in Charge of OIG's Special Investigations Branch requesting that it investigate the allegations in the GE Letter. On May 18, 2010, OIG responded that it would take no action because the referral lacked evidence of criminal conduct and noting that the disclosures implicated the WPA.¹² In the meantime, FDA

¹² On June 28, 2010, after Spector had been installed on Scientist 2's computer and 2 days before it would be installed on the remaining scientists' computers, CDRH renewed its request that OIG open an investigation, on the basis of evidence it gathered during its computer monitoring, including "documents suggesting that employees are engaged in the inappropriate, and likely illegal, disclosure of nonpublic information." In response, OIG opened an investigation on July 31, 2010, and, after completing its review, presented the matter to the U.S. Department of Justice, where prosecutors reviewed the matter and declined prosecution. By letter dated November 15, 2010, OIG notified the CDRH Director that it had closed its investigation, noting that prosecutors declined prosecution and "[y]our 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."

had already initiated its monitoring of Scientist 1 (OIM installed Spector on Scientist 1's laptop on April 22, 2010).¹³

On May 17, 2010, FDA used EnCase for the first time to obtain a snapshot of the contents of Scientist 1's computer hard drive and attached external memory devices. For example, CNI staff recalled an EnCase analysis it performed of a non-FDA thumb drive belonging to Scientist 1 that was plugged into an FDA computer. However, it appears EnCase also was used to conduct searches unrelated to anything identified through Spector. Additional EnCase snapshots were taken several times before the writing of the Draft OGC Memo.

The Interim Report of Investigation

On or about June 3, 2010, the CNI Team Member authored a summary of the computer monitoring captioned "Subjects of Interest," which he transmitted to FDA's CIO under a cover memo captioned, "Interim Report of Investigation." The cover memo characterized the allegations presented to the FDA Security Department as follows:

- "Ghost writing HIS subordinates' reports, in particular those surrounding those reports that are identified by the letter 'K' followed by six (6) numbers."
- "[Scientist 1] 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 cover memo added that "[t]he analytical findings to date appear to support the allegations, however the review is ongoing and substantial volumes of data are currently being culled."

The report summarized data and communications identified by looking at 2 weeks' worth of Spector screen shots. The report contained four categories of "subjects": primary, secondary, ancillary, and media outlet. The "primary" subjects were individuals within FDA with the highest frequency of communication regarding improper release of confidential information or ghostwriting. The "secondary" subjects referred to individuals within the agency with substantive communications about the search term issues at any frequency level. "Ancillary" subjects referred to individuals outside the agency with any communications about the search term issues and included a Member of Congress and Congressional staff. "Media outlet" subjects referred to members of the media with any communications about the search term

¹³ A draft Office of the General Counsel (OGC) legal memorandum (Draft OGC Memo), discussed more fully below, mistakenly asserts that CDRH began its computer monitoring of Scientist 1 after OIG's May 18, 2010, response.

issues. This report did not indicate—and we found no evidence—that the monitoring was implemented in a manner specifically designed to capture communications with Congress, as has been alleged to HHS.

The report characterizes the primary subjects (Scientist 1, Scientist 2, and a former CDRH employee) as follows: “The above listed subjects appear to be the point men. All communications amongst all the subjects filter through one or all of these three primary subjects.”

Scientist 3, Scientist 4, and Scientist 5 were included on the list of secondary subjects; the report summarizes their communications as follows:

The secondary subjects listed above are in constant communication amongst themselves and the primary subjects 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.

The report included hyperlinks labeled “View All instances of the above noted in order by date” that linked to screen shots showing some of the data the report identified.

Computer Monitoring of Additional Scientists Begins

Partly on the basis of information discovered while monitoring Scientist 1, including email contacts between Scientist 1 and others, CDRH’s Executive Officer told OIM staff to expand the monitoring, and Spector then was installed on additional FDA computers used by Scientist 2 (on May 24, 2010) and Scientist 3, Scientist 4, and Scientist 5 (all on June 30, 2010).

According to CDRH’s Executive Officer, the decision to expand the monitoring was a group decision made by her, the CIO, the Assistant Commissioner for Management, CDRH’s then Associate Director, Office of In Vitro Diagnostic Device Evaluation and Safety, and others.¹⁴ We found no evidence that this group considered employing any investigative technique other than computer monitoring.

On June 25, 2010, an OGC attorney discussed expanding the monitoring in an e-mail to FDA’s Chief Counsel. “[Attorney to attorney communication redacted.]”

In the CDRH Director’s June 28, 2010, letter to OIG (discussed in footnote 11 above), the CDRH Director described what was discovered during the monitoring:

¹⁴ CDRH’s then Associate Director, Office of In Vitro Diagnostic Device Evaluation and Safety, disputed her involvement in computer-monitoring decisions, stating she did not know who at FDA was being monitored.

“Specifically, [the documents discovered during the computer monitoring] show that the employee at issue and other employees have recently disclosed nonpublic information to at least one former FDA employee.... We have also discovered e-mails that the employee in question sent to unauthorized recipients which appear to have attachments likely containing confidential commercial information....”

A July 25, 2010, email from the CDRH Director to the Deputy FDA Commissioner stated:

...after several weeks of monitoring IT security and FDA technical experts identified several instances in which [Scientist 1] provided confidential information about medical devices under review to [a former FDA scientist] when [that former FDA scientist] was no longer an FDA employee. In some instances the medical devices did not pertain to [this former FDA scientist's] area of expertise. Other CDRH employees were participants in these email exchanges. As a result, FDA expanded its monitoring to the computers of four other CDRH staff who were parties to the disclosure of confidential information.

Procedures Used During FDA's Computer Monitoring

As discussed above, screen shots that CNI staff identified as showing potential indications of ghostwriting or unauthorized disclosures were shared with CDRH's then Associate Director, Office of In Vitro Diagnostic Device Evaluation and Safety, for further review. The then Associate Director also made written lists of filenames of monitored emails and screen shots that appeared to contain CCI or details of internal processes being sent outside the FDA computer network and gave these lists to CDRH's Executive Officer asking her to confirm with FOIA experts whether the information identified as CCI was actually CCI. The then Associate Director identified some of the emails as going to individuals who no longer worked for FDA, as well as Members of Congress; when she talked to the CDRH Director about information going outside FDA, he expressed his understanding that employees have the right to share CCI with the press if they think there are immediate, urgent public health concerns that are being ignored by FDA.

As with Scientist 1, FDA used EnCase to take images of the other scientists' computers and network memory several times, usually in an attempt to recover something seen on a Spector screen shot. For instance, CNI staff used EnCase after it observed that numerous potential FDA files were being copied and transferred to a thumb drive docked into Scientist 3's FDA computer (when a thumb drive is docked into an FDA asset, the thumb drive becomes part of the FDA network).

FDA Consultations With OGC

With no agency policies in place, FDA and CDRH officials had no written guidance to follow to ensure that any computer monitoring would be conducted in accordance with applicable laws and in a manner that protected the rights of employees.¹⁵ We found no evidence of consultation between FDA and OGC prior to the decision to conduct computer monitoring of Scientist 1 in April 2010. FDA stated that after monitoring began, OGC was consulted on a June 2010 draft referral from CDRH to OIG on issues related to computer monitoring. Also in approximately June 2010, a staff attorney in the OGC Food and Drug Division (FDD), at the direction of the Associate General Counsel of FDD, wrote a legal memorandum (the Draft OGC Memo), which addressed some of the legal issues raised by the computer monitoring.¹⁶

The Draft OGC Memo is relevant to our review, even though the latest version of it was dated July 8, 2010—several weeks after the initiation of the computer monitoring of Scientist 1—because it is the only document from an attorney provided to OIG evidencing FDA’s and CDRH’s understanding of the applicability of legal limits on the conduct of searches of Government employees. The legal advice provided in the memorandum was limited in scope and did not address the applicability of all the relevant laws to all the targeted scientists.

CDRH Takes Action as a Result of Monitoring

As a result of the information collected during the monitoring, Scientist 1 was put on administrative leave on July 7, 2010, and his term appointment expired on July 31, 2010. Scientist 4 was given advance notice of removal from Federal service on December 6, 2010, for unauthorized release of agency information; however, Scientist 4 was temporarily reappointed on February 17, 2012, and her reappointment remained effective through September 25, 2013. Scientist 3’s appointment was not renewed as of November 6, 2010. Scientist 2, who was a Commissioned Corps officer, was directed to nonduty with pay status on May 5, 2011, and was formally terminated from the Commissioned Corps on October 9, 2011. Scientist 5 remains employed by CDRH.

¹⁵ FDA published and periodically updated a *Forensic & Incident Response Procedures Manual*; however, this manual is a technical document largely based on technical guidance from the Department of Commerce’s National Institute for Standards and Technology. It does not provide guidance to FDA managers on how to conduct investigations, office searches, or computer monitoring.

¹⁶ According to FDA, the Draft OGC Memo was never finalized. FDA told us that it does not know why it was not finalized and that, since the Associate General Counsel of FDD (who directed preparation of that memorandum) no longer works in OGC, FDA would speculate as to neither the reasons for directing preparation of it nor the way in which it was used. During our review, OIG saw several iterations of this memorandum. The Draft OGC Memo is marked “privileged and confidential – attorney work product.”

In four letters sent in March and April 2011, CDRH wrote to companies with business at CDRH to inform them that CDRH had determined that one of its Office of In Vitro Diagnostics employees had made unauthorized disclosures of their CCI in July or August 2010 via email. In each letter, CDRH apologized and made assurances that it had taken appropriate administrative action.

II. FINDINGS

We found that CDRH had reasonable concern that confidential information, including possibly trade secrets and/or CCI, had been disclosed by agency employees without authorization. This concern was reasonable largely because news reports cited internal agency documents and agency scientists as sources of the confidential information. Indeed, by the spring of 2011, CDRH was sufficiently certain that its investigation had turned up evidence of such unauthorized disclosures that it sent letters of apology to several device manufacturers.

We also found that FDA had provided notice to its scientists (and all other users of its network) through a network log-on banner that there was no right to privacy on the FDA computer network and that all data on the network were subject to interception by FDA. Consistent with the banner, FDA monitored the scientists' communications over FDA's network using computer-monitoring technology that captured communications from both their Government and personal email accounts. In our interviews of those conducting the computer monitoring and our review of other data sources, we found no evidence that FDA had obtained or used passwords to any of the scientists' private email accounts, nor did we find any evidence that FDA logged into any of the scientists' computers in order to gain live access as a user of the computer. The images of private emails that FDA obtained were captured by screen shots taken by Spector of the scientists' use of the FDA network.

Because there was no policy in place at FDA or CDRH to ensure compliance with applicable laws and restrictions, such as the Fourth Amendment, Title III, and the WPA, it was particularly important for FDA and CDRH to ensure that it understood the full extent of the limits on the agency and the rights of its employees. However, we found no evidence that FDA or CDRH planned its investigation or scoped the monitoring with the timely assistance of counsel, who could have advised FDA and CDRH prior to the monitoring on compliance with relevant requirements, such as the Fourth Amendment, criminal prohibitions on the interception of electronic communications, and the WPA; there was no policy in place at FDA or CDRH to ensure compliance with these requirements.

The legality of the surveillance under these authorities currently is being litigated, and we are not prejudging the outcome. Nevertheless, we find that despite the reasonableness of CDRH's concerns and the explicit language in FDA's network banner, CDRH should have

assessed beforehand, and with the assistance of legal counsel, whether potentially intrusive EnCase and Spector monitoring would be the most appropriate investigative tools and how to ensure that the use of these tools would be consistent with constitutional and statutory limitations on Government searches.

For instance, in the absence of existing guidance, CDRH should have considered, and sought legal counsel on, the following in advance of the monitoring:

1. Did the leaked information implicate criminal prohibitions or merely regulatory ones? (This question is relevant to both the permissibility of the monitoring under the Fourth Amendment and to the applicability of the WPA. See Appendix C.)
2. Was FDA's network log-on banner sufficient to remove all the scientists' REP, and would the use of EnCase or Spector constitute a search that was justified at its inception and that was of permissible scope?¹⁷
3. Were the five scientists whistleblowers under the WPA, and if so, how should the surveillance be conducted to ensure that there would be no WPA-prohibited retaliation?¹⁸
4. Was Title III applicable, and if so, did the surveillance fall under an applicable exception?

We found no evidence that CDRH or FDA considered these legal questions before initiating surveillance. The only documented legal analysis, namely the Draft OGC Memo, was prepared after the surveillance already had begun. While recognizing that the Draft OGC Memo was just that—a draft—it is one of few indications of any contemporaneous consultation with, or consideration by, FDA counsel.

Another indicator of the lack of adequate consideration of the implications of the Fourth Amendment, in particular, is the lack of documentation supporting both the reasons why EnCase and Spector—both of which broadly capture information—were determined to be the most appropriate tools and the manner in which the EnCase and Spector searches were scoped. Specifically, we found that the discussion of what investigative technique to use and how to scope the monitoring was limited largely to technical discussions with information technology

¹⁷ Courts have established that a sufficiently broad network banner can eliminate a Government employee's REP. It is important to note, however, that soon after FDA began its computer monitoring, the United States Supreme Court decided *City of Ontario v. Quon*, in which the Court's Fourth Amendment analysis bypassed the question of REP altogether and concluded the search was legal after applying the two-part test that the search be justified at its inception and permissible in scope. This suggests that a prudent agency would ensure that any monitoring would be of permissible scope under *O'Connor v. Ortega* (see Appendix C), even in cases when the monitored employee has no REP.

¹⁸ In the wake of revelations about FDA's monitoring of its scientists, the Office of Special Counsel (OSC) issued guidance to Federal agencies stating that "agency monitoring specifically designed to target protected disclosures to the OSC and IGs is highly problematic."

professionals about the available surveillance technology. In addition, neither CDRH nor FDA's OIM staff could produce or recall the substance of the specifications on how to implement the Spector monitoring that were provided by the CNI Team Leader to his subordinate conducting the monitoring. Similarly, although OIG was able independently to identify search terms applied when CDRH used EnCase to search for relevant material on the scientists' computers, we found no document that explained the relevance of these search terms. The absence of documentation concerning scoping decisions makes it difficult to evaluate the reasonableness of these computer searches.

Because CDRH and FDA did not prospectively assess the relative risks involved in whether or how to conduct investigations of potential whistleblowers, such as ensuring that their investigations were conducted in accordance with laws and regulations, the computer monitoring of the five scientists had significant negative consequences for FDA. A timely, fuller, and better documented consideration of all of these risks may have provided the agency greater protection from controversy, while demonstrating the agency's commitment to protecting its employees' rights.¹⁹

III. RECOMMENDATIONS

HHS should ensure that its operating divisions (OpDivs) draft and implement policies and related procedural internal controls that provide reasonable assurance of compliance with laws and regulations, particularly those governing current and prospective employee monitoring. At a minimum, the internal controls concerning electronic monitoring of employees²⁰ should address:

- the agency's authority to monitor employee communications or access employee files;
- protection of the rights of employees and the extent of an employee's expectation of privacy while using agency IT resources;
- specific conditions for requesting access to employee communications;
- defined roles and responsibilities for initiating, reviewing, and approving requests to access employee communications and data; and

¹⁹ On June 17, 2013, all HHS employees received an email both describing the Department's authority and ability to monitor the electronic activities that take place on its networks and equipment and notifying employees of the laws in place to protect Federal employees who reveal instances of waste, fraud or abuse within the Federal Government, commonly referred to as the "Whistleblower Protections laws." The email included a notice regarding the Whistleblower Protection Enhancement Act of 2012.

²⁰ This includes, but is not limited to, current and former Federal employees, contractors, interns, and visitors that are provided access to HHS information technology and data.

- retention of records that document the initiation, review, and approval of electronic monitoring, including opinions and recommendations of legal counsel.

At the time of FDA's investigation of the five scientists, neither the Department, FDA, nor CDRH had policies or procedures in place that governed the monitoring of agency employees' use of Government IT resources. After public revelations that FDA had monitored its employees, HHS implemented a Department-wide policy regarding such computer surveillance. Issued on June 26, 2013, HHS's "Policy for Monitoring Employee Use of HHS IT Resources" requires that its agencies "establish policies and procedures that will strengthen the ability to effectively document, analyze, authorize, and manage requests for HHS employee computer monitoring." The policy states that "[w]hile the warning banner gives OpDivs the authority to monitor employee use of IT resources, it is each OpDiv's responsibility to carry out monitoring in a fashion that protects employee interests and ensures the need for monitoring has been thoroughly vetted and documented." The policy gave the agencies, including FDA, 90 days to develop and deliver written policies and procedures that meet requirements laid out in the HHS policy. These requirements include, among other things: maintaining advanced written authorization of any computer monitoring, consulting with OGC to ensure the proposed monitoring complies with all legal requirements, and documenting the basis for approving requests to conduct computer monitoring.

FDA issued its interim computer-monitoring policy on September 26, 2013. In particular, the FDA's interim policy:

- establishes procedures requiring authorization by senior management and consultation with legal counsel;
- distinguishes between monitoring conducted at the behest of law enforcement and monitoring conducted for management purposes to minimize interference with law enforcement investigations;
- requires monitoring to be narrowly tailored in time, scope, and degree to accomplish the monitoring's objectives; and
- requires that the authorization describe the reason, factual basis, and scope of the monitoring.

Given this, FDA's interim policy addresses our five recommendations outlined above.²¹ HHS should determine whether all other individual OpDiv policies meet our recommendations above. HHS also should regularly review and, as necessary, update its Department-wide

²¹ We note that both the HHS policy and the FDA policy are ambiguous with respect to their applicability to circumstances in which the misconduct being investigated might not violate a written policy. HHS and FDA should ensure that their managers have adequate guidance in such cases.

monitoring policies to ensure they are compatible with new and emerging technologies and methodologies. Information technology is continually changing, and a static monitoring policy could fail to address key implementation issues as capabilities evolve.

IV. DEPARTMENT RESPONSE

HHS concurred with all of the recommendations in this report. See Appendix D for the full text of HHS's comments. HHS also offered technical comments that we incorporated as appropriate.

APPENDIX A: Methodology

This review was conducted by a 12-member team (the Review Team) composed of individuals from OIG's Immediate Office, Office of Audit Services, Office of Counsel to the Inspector General, Office of Evaluation and Inspections, Office of Investigations, and Office of Management and Policy.

We interviewed current and former employees of FDA for this report, including the CDRH Director, the CDRH Executive Officer, the then Associate Director in CDRH's Office of In Vitro Diagnostic Device Evaluation and Safety, the FDA OCI Office of Internal Affairs SAC, an OCI Office of Internal Affairs Assistant SAC, and FDA's former Chief Information Security Officer during the relevant time period. We also interviewed two employees of CNI, an FDA contractor: the CNI Team Leader and the CNI Team Member.

We were unable to interview certain individuals with information relevant to our review. FDA's former CIO, who is no longer in Federal service, declined through counsel to speak with the Review Team. Similarly, an attorney collectively representing the five scientists subject to computer monitoring did not respond to our repeated information requests.

The Review Team also collected information and documents from FDA on topics that included policies regarding the use of software to engage in computer surveillance of FDA employees, surveillance software files and logs, and consultations FDA engaged in prior to initiating monitoring. In all, we received more than six terabytes of information that included documents, emails, and screen shots.

Throughout this document, when an assertion is made, it is based on information gathered from witness interviews and other evidence reviewed by the Review Team.

APPENDIX B: CDRH and the Premarket Application Process

CDRH is responsible for ensuring the safety and effectiveness of medical devices. Devices vary in complexity and application, ranging from simple tongue depressors to complex pacemakers. CDRH assigns each type of device one of three regulatory classifications (Class I, II, or III), which are based on the level of control needed to ensure the safety and effectiveness of the device for patients and other end users. Regulatory control increases from Class I to Class III. A device's risk classification determines its premarket review process.²²

CDRH must approve Class III medical devices prior to their marketing under either the Premarket Approval process or the Premarket Notification (the latter is referred to as "510(k)") process. Premarket Approval review is the most stringent process for obtaining FDA approval to market a device and is required by statute for devices that support or sustain human life, are of substantial importance in preventing impairment of human health, or present a potentially unreasonable risk of illness or injury.²³

If a Class III device is not required to undergo Premarket Approval, the manufacturer must submit to CDRH a 510(k) application. The 510(k) is a faster and less stringent premarket review process than Premarket Approval. Submissions under the 510(k) process must demonstrate that a device to be marketed is substantially equivalent to a predicate device that is already legally marketed in the United States.²⁴ CDRH determines a device is substantially equivalent to a predicate device if the 510(k) submission demonstrates that it has the same intended use and technological characteristics as the predicate. A device with technological characteristics that differ from the predicate device may also be declared substantially equivalent if the information in the 510(k) submission demonstrates that the device is at least as safe and effective as the predicate and does not raise new questions of safety and effectiveness.²⁵

Scientists who are either CDRH staff or contract employees determine which regulatory class a device falls into, whether a device should be reviewed under the Premarket Approval or 510(k) process, and whether a device should be approved, or cleared.

²² See 21 C.F.R. § 860.3.

²³ See the Federal Food, Drug, and Cosmetic Act §§ 515(a) and 513(a)(1)(C), 21 U.S.C. §§ 360e(a) and 360c(a)(1)(C).

²⁴ See 21 CFR § 807.92(a)(3).

²⁵ FDA, CDRH, *Guidance on the CDRH Premarket Notification Review Program 6/30/86 (K86-3)*, 510(k) Memorandum #K86-3.

APPENDIX C: Applicable Legal Criteria

The FDA scientists' communications with outside entities and FDA's computer monitoring implicate a variety of legal restrictions relating to disclosure of information and to privacy. This appendix summarizes those legal principles, which are relevant to determining whether the conduct of the FDA scientists provided a sufficient legal basis for FDA to engage in the computer monitoring in the manner and scope that it did.

Reasonableness of a Computer Search

The Fourth Amendment's protections against unreasonable searches and seizures apply where an individual has REP. Without REP, a search by the Government is not a search for the purposes of the Fourth Amendment. Where there is REP, the Government generally must have probable cause and obtain a warrant for a search to be reasonable. In general, Government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no REP in the information stored there.

The Supreme Court's decision that governs the constitutionality of a search in a government office is *O'Connor v. Ortega*, 480 U.S. 709 (1987). In *Ortega*, the Supreme Court describes the factors for determining REP:

Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.

Ortega, 480 U.S. at 717.

Therefore, whether the scientists had REP in their use of FDA computer resources — such as computer hard drives, external memory devices, and network storage — is determined on a case-by-case basis and will be influenced by such facts as the presence and wording of FDA's network banner.

Where a public employee has REP, there are several exceptions to the probable cause and warrant requirements. Among these is the exception for workplace searches conducted for purposes unrelated to the enforcement of criminal laws. The Supreme Court held in *Ortega* that “public employer intrusions on the constitutionally protected privacy interests of government

employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.” Further, the search must be justified at its inception and permissible in scope. A search is justified at its inception if there are reasonable grounds, based on all of the circumstances, for suspecting that the search will (1) turn up evidence that the employee engaged in work-related misconduct or (2) that the search is necessary for a noninvestigatory work-related purpose, such as to retrieve a file when the employee is not available. It is permissible in scope where the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct. *Ortega*, 480 U.S. at 726. The measures, however, need not be the least intrusive measures practicable.²⁶

It is important to note that in one of the Supreme Court’s recent consideration of a workplace search of a Government employee’s use of agency information resources, the Court avoided the question of REP altogether and proceeded to apply the two-part test that the search must be justified at its inception and permissible in scope.²⁷ Because of the uncertain or speculative nature of REP determinations, application of the two-part test in all circumstances prior to the initiation of a workplace search, such as computer surveillance, could help limit the Government employer’s litigation vulnerability.

Interception of Electronic Communications

FDA’s computer monitoring potentially implicates criminal prohibitions on the interception or acquisition of electronic communications without process because Spector captured images of e-mails being prepared or dispatched by the scientists using both their personal and FDA e-mail accounts. Title III, as amended by the Electronic Communications Privacy Act of 1986, governs the authority of the Government to intercept electronic communications, such as email. Title III requires that the Government obtain a court order prior to engaging in real-time interception of email, as would be required for real-time interception of telephone calls. Among the exceptions to the court order requirement is the “consent exception,” which requires an analysis similar to establishing whether REP exists. In particular, the consent exception analysis would be used to determine whether an individual gave consent by agreeing to abide by the terms of FDA’s computer network banner when logging onto FDA’s network.

The law also limits the Government’s ability to obtain “stored communications.” Amendments made to Title III by the Stored Communications Act require the Government to issue a subpoena to an email service provider to acquire emails that have been retrieved by the

²⁶ See *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010).

²⁷ *Quon*, 130 S. Ct. at 2630.

holder of the email account. To acquire emails that have not been retrieved, the Government must either issue a subpoena or obtain a warrant depending on how long the email has been in electronic storage with the email service provider. These provisions are relevant only if FDA acquired stored personal emails from the five scientists' email service providers.

The Whistleblower Protection Act

Although a workplace search may be justifiable under existing Fourth Amendment principles and under Federal prohibitions on disclosure of information, searches conducted against those who make disclosures to, for example, Congress or to the press may implicate the prohibition in the WPA, at 5 U.S.C. § 2302, against retaliation.

Subsequent to public revelations of the FDA's surveillance of its five employees, OSC issued a memorandum in which it stated that "agency monitoring specifically designed to target protected disclosures to OSC and IGs is highly problematic." This admonition was based in part on the provisions of the WPA, which prohibit taking or not taking any personnel action with respect to a Government employee because of any disclosure of information that the employee reasonably believes to evidence violations of law or regulation, waste and abuse, or a specific danger to public health. Section 2302 defines "personnel action" to include disciplinary or corrective actions or any other significant change in working conditions and is therefore sufficiently broad to include targeting an employee for computer surveillance. Notably, the statute does not specify to whom a disclosure must be made for whistleblower protections to be available, and thus the statute has been interpreted to cover disclosures made to media outlets, in addition to OIGs, OSC, and Congress.²⁸

Section 2302 contains one important caveat regarding the applicability of whistleblower protections: an agency is prohibited from taking (or not taking) a personnel action only when the disclosure made by the employee is not specifically prohibited by law. Therefore, the statutory prohibitions on certain disclosures, described immediately below, are relevant to the applicability of this caveat to FDA's monitoring of its employees.

Prohibitions on the Disclosure of Information by FDA Employees

Several statutory and regulatory provisions limit the ability of FDA employees to share agency information with others outside the agency. Violation of any of these provisions may provide a legitimate basis for an internal investigation. The Federal criminal statute generally

²⁸ See e.g., *Horton v. Department of the Navy*, 66 F.3d 279 (Fed. Cir. 1995) (stating, "The purpose of the Whistleblower Protection Act is to encourage disclosure of wrongdoing to persons who may be in a position to act to remedy it, either directly by management authority, or indirectly as in disclosure to the press.").

limiting disclosures, at 18 U.S.C. § 1905, provides for removal and for criminal penalties for the disclosure of trade secrets and confidential business information where such disclosure is not authorized by law. The Federal Food, Drug, and Cosmetic Act has additional criminal provisions at 21 U.S.C. §§ 331(j) and 333, which prohibit the disclosure of trade secrets (but not confidential business information) submitted to the FDA in accordance with FDA approval processes. The prohibition in section 331(j) does not apply to disclosures made to Congress or its committees, but it does apply to disclosures to the media. FDA implemented and expanded on section 331(j) in its regulation at 21 CFR § 20.61. The regulation states that neither trade secrets nor CCI is available for public disclosure outside of the procedures set forth in the regulation and provides definitions for “trade secrets” and “CCI.”

Finally, FDA has implemented disclosure restrictions with respect to PMAs. “The existence of a PMA file may not be disclosed by FDA before an approval order is issued to the applicant unless it previously has been publicly disclosed or acknowledged.” 21 CFR § 814.9. Furthermore, “If the existence of a PMA file has not been publicly disclosed or acknowledged, data or information in the PMA file are not available for public disclosure.” Similarly, 21 CFR § 807.95 prohibits the disclosure of the existence of a PMA, except under the specified circumstances.

Appendix D: Department Comments



THE SECRETARY OF HEALTH AND HUMAN SERVICES
WASHINGTON, D.C. 20201

February 24, 2014

To: Daniel R. Levinson
Inspector General
U. S. Department of Health and Human Services

Subject: Response to OIG Draft Memorandum Report: *Review of the Food and Drug Administration's Computer Monitoring of Certain Employees in Its Center for Devices and Radiological Health*, OIG-12-14-01

On July 20, 2012, I requested the Office of the Inspector General (OIG) to conduct a review of the Food and Drug Administration's Center for Devices and Radiological Health employee monitoring practices. OIG conducted this review and, on January 24, 2014, issued the OIG Draft Memorandum Report: *Review of the Food and Drug Administration's Computer Monitoring of Certain Employees in Its Center for Devices and Radiological Health*, OIG-12-14-01.

The Draft Memorandum Report requested comments pertaining to the recommendations in the report. I have reviewed this report and concur with the OIG recommendations, as described in the attachment provided by my office.

Please do not hesitate to reach out to me, E. J. Holland, Assistant Secretary for Administration, David Horowitz, Deputy General Counsel, or Frank Baitman, Chief Information Officer, if you have any questions or need additional information.

Kathleen Sebelius

Enclosure: Attachment: Responses to Recommendations in OIG Draft Memorandum Report
OIG-12-14-01

Appendix D, continued

Attachment: Responses to Recommendations in OIG Draft Memorandum Report OIG-12-14-01

The U.S. Department of Health and Human Services (HHS) is in receipt of the Office of Inspector General's (OIG) draft report entitled "*Review of the Food and Drug Administration's Computer Monitoring of Certain Employees in its Center for Devices and Radiological Health, OIG 12-14-01.*" Our concurrence with the recommendations in this report shall not be construed as a waiver by HHS of any privileges or exemptions from disclosure that HHS may assert in any proceedings with respect to any information or records referenced in the document.

OIG RECOMMENDATIONS:

I. HHS should ensure that its Operating Divisions (OpDivs) draft and implement policies and related procedural internal controls that provide reasonable assurance of compliance with laws and regulations, particularly those governing current and prospective employee monitoring. At a minimum, the internal controls concerning electronic monitoring of employees should address:

- the agency's authority to monitor employee communications or access employee files;
- protection of the rights of employees and the extent of an employee's expectation of privacy while using agency IT resources;
- specific conditions for requesting access to employee communications;
- defined roles and responsibilities for initiating, reviewing, and approving requests to access employee communications and data;
- retention of records that document the initiation, review, and approval of electronic monitoring, including opinions and recommendations of legal counsel; and
- maintaining advanced written authorization of any computer monitoring, consulting with the OGC to ensure the proposed monitoring complies with all legal requirements, and documenting the basis for approving requests to conduct computer monitoring.

HHS RESPONSE: CONCUR

As noted in the OIG Draft Memorandum Report OIG-12-14-01, HHS issued the *Policy for Monitoring Employee Use of HHS IT Resources* Memorandum on June 26, 2013. This memorandum instructed the OpDivs to develop and implement policies and procedures that incorporated the requirements listed above. A copy of the memorandum was posted on the HHS Whistleblower webpage¹ and the Office of the Chief Information Officer (OCIO) webpage². On June 26, 2013, an email was sent from the HHS Assistant Secretary for Administration (ASA) through the HHS CIO to HHS OpDiv Heads, StaffDiv Heads, and Executive Officers, informing them of the memorandum. The following day, the HHS Chief Information Security Officer (CISO) also notified the OpDiv CISOs of this new policy

¹ <http://intranet.hhs.gov/hr/whistleblower.html>

² <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>

Appendix D, continued

requirement. During the following months, the HHS CISO communicated with the OpDiv CISOs at their monthly Council meeting to ensure that progress was made in the development of their new policies.

HHS agrees that with the recommendation that the OpDivs implement policies and procedures that provide reasonable assurance of compliance with laws and regulations. HHS also agrees that the OpDiv policies and procedures should address the elements highlighted by OIG, which are incorporated in the HHS memorandum of June 26, 2013.

2. HHS should determine whether all other individual OpDiv policies meet our recommendations outlined above.

HHS RESPONSE: CONCUR

HHS agrees that the HHS CIO should determine whether individual OpDiv policies comply with the essential elements of the HHS policy, which are in accordance with the OIG recommendations outlined above. The HHS CISO Policy Team has initiated a process to track and review current OpDiv computer monitoring policies and procedures. HHS is actively working with OpDivs, as needed, to further refine their policies and procedures.

3. HHS also should regularly review and, as necessary, update its Department-wide monitoring policies to ensure they are compatible with new and emerging technologies and methodologies. Information technology is continually changing, and a static monitoring policy could fail to address key implementation issues as capabilities evolve.

HHS RESPONSE: CONCUR

HHS agrees that regular review and updating of the computer monitoring policies and procedures is essential. HHS CISO will ensure that each OpDiv periodically reviews and updates its policies and procedures to ensure that they reflect implementation experience and stay in alignment with any relevant changes in technology, law and policy.



**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

I.	Table of Contents	2
II.	Table of Names	3
III.	Executive Summary	5
IV.	Findings	9
V.	Recommendations	11
VI.	Background	12
A.	Confidential Documents are Posted Online	16
VII.	Authorization and Instructions for Monitoring	17
VIII.	Details of the Computer Monitoring	25
IX.	Evolution of the Monitoring Program	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
X.	The Office of Inspector General Declines to Investigate	39
XI.	Monitoring Was Not the Solution	41
XII.	Managing By Investigation	42
XIII.	Post-Monitoring Changes	45
XIV.	Conclusion	47
XV.	Appendix I: Relevant Documents	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.

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.⁸ 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.⁹ 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.¹⁰ 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.¹¹ The report described information found on Dr. Smith’s computer, including e-mails with journalists, Congress, and the Project on Government Oversight.¹² The report also stated that Dr. Smith “ghostwrote” reports for his subordinates and supplied internal CDRH documents to external sources.¹³ After receiving this report, the FDA expanded the computer monitoring to include three additional CDRH scientists¹⁴ and declined to renew Dr. Smith’s contract.¹⁵

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.¹⁶ The OIG declined these requests, noting that contacts with the media and Congress were lawful, and no evidence of criminal conduct existed.¹⁷ 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.¹⁸ However, the FDA failed to take direct administrative or management action on its own to address the concerns directly.

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

⁹ *Id.*

¹⁰ 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].

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ McKee Tr. at 16.

¹⁵ *Id.* at 33.

¹⁶ 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].

¹⁷ 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].

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

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.¹ 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.²

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.³ Additionally, Dr. Smith and his colleagues reported allegations of retaliation to Congress and the U.S. Office of Special Counsel (OSC).⁴

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.⁵ Approximately one month later, the monitoring expanded to another CDRH scientist.⁶ Using a software monitoring program called Spector 360, which took screenshots of FDA employees' computers every five seconds,⁷ FDA officials were able to obtain sensitive information and protected communications, including attorney-client

¹ 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 (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).

² 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*].

³ *Scientists Complain to Obama*, *supra* note 1.

⁴ 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*].

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

⁶ 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*].

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

FDA officials eventually forwarded information gathered from the computer monitoring program to the OIG.¹⁹ 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.²⁰ In November 2010, by letter, the Criminal Division formally declined to take up the matter.²¹

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.²²

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

¹⁹ 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].

²⁰ Shuren Tr. at 67-68.

²¹ 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].

²² *Id.*

chills whistleblower communications with Congress, the OSC, and Inspectors General.²³ 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.

²³ 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.²⁴
- 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.

²⁴ 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.²⁵ Specifically, the FDA is charged with regulating and supervising a variety of consumer health products.²⁶ These products include dietary supplements, prescription and over-the-counter drugs, vaccines, biopharmaceuticals, and medical devices.²⁷ The FDA has broad powers for determining the safety, risks, marketing, advertising, and labeling of these products.²⁸

The Center for Devices and Radiological Health (CDRH) is a division within the FDA.²⁹ The CDRH is also tasked with protecting and promoting public health.³⁰ 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.³¹ The CDRH tests and examines potential medical devices, and makes recommendations to the FDA regarding the approval and widespread usage of radiation-emitting products.³² The CDRH seeks to assure consumer confidence in devices manufactured in the United States.³³ 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.³⁴

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.³⁵ 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.³⁶ 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.³⁷ In an attempt to implement more stringent guidelines for this

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

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

²⁷ *Id.*

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

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

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

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

³⁴ *Id.*

³⁵ CDRH Letter, *supra* note 4.

³⁶ *Id.*

³⁷ *Id.*

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

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.”⁴¹ The article further stated that “an agency supervisor improperly forced them to alter reviews of [a] breast imaging device.”⁴² The article, citing internal FDA documents, referred specifically to the ongoing review of the iCAD SecondLook Digital Computer-Aided Detection System for Mammography device.⁴³ 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.”⁴⁴

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.⁴⁵ 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

³⁸ 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.

³⁹ 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).

⁴⁰ CDRH Letter, *supra* note 4; NWC Letter, *supra* note 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).

⁴¹ *Rush to Approve Devices*, *supra* note 1.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

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

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

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

On October 1, 2009, Dr. Jeffrey Shuren, Director of the CDRH, talked to a reporter about a different medical device.⁵¹ Dr. Shuren learned that the reporter was also in possession of similar documents related to the pre-market medical device process.⁵² 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.⁵³

⁴⁶ *Id.*

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

⁴⁸ Ferry Letter, *supra* note 45.

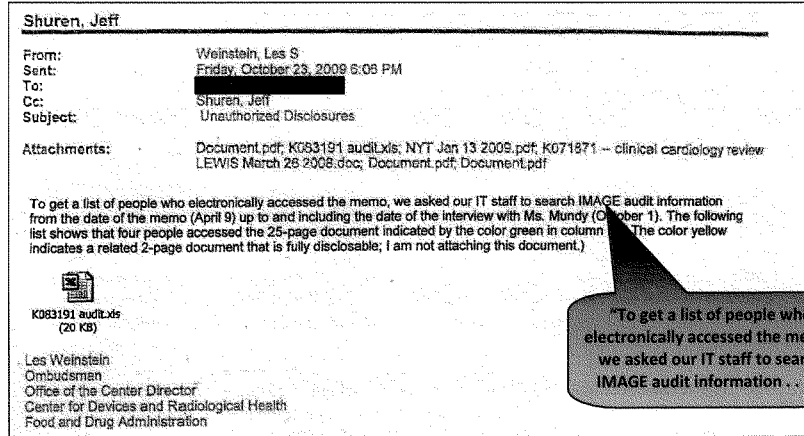
⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ Weinstein E-mail, *supra* note 16.

⁵² *Id.*

⁵³ *Id.*



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

On March 28, 2010, the *New York Times* published a second article regarding the FDA's approval process for medical devices.⁵⁶ 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.⁵⁷

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.⁵⁸ 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.⁵⁹

⁵⁴ *Id.*

⁵⁵ Shuren Tr. at 14.

⁵⁶ *F.D.A. Ignored Radiation Warnings*, *supra* note 2.

⁵⁷ *Id.* (emphasis added).

⁵⁸ 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.⁶⁰ Included in these materials were confidential and proprietary FDA documents, as well as confidential communications between FDA employees and Congress, OSC, and personal attorneys.⁶¹ 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.⁶²

After the documents left FDA, they followed a chain of custody that included several parties before they got to QAI.⁶³ According to HHS, QAI received the job from PSC on May 2, 2012, and completed it on May 9, 2012.⁶⁴ The files were uploaded to the site at the direction of PSC, on May 3, 2012.⁶⁵ They were removed from the site and archived six days later on May 9, 2012.⁶⁶ During this time, confidential and proprietary information was publically available and easily searchable.⁶⁷

QAI officials claimed they were simply following their client's instructions.⁶⁸ In fact, FDA did not mark the documents as confidential, and there is no written record reflecting the sensitive nature of the documents.⁶⁹ 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.⁷⁰ 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.⁷¹ HHS identified the misclassification as a "clerical error at the PSC."⁷²

⁵⁹ *Id.*

⁶⁰ 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].

⁶¹ NWC Letter, *supra* note 4.

⁶² Esquea Letter, *supra* note 60.

⁶³ *Id.*

⁶⁴ *Id.*

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

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *See id.*; *see also* Esquea Letter, *supra* note 60.

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

⁷¹ *Id.*

⁷² Esquea Letter, *supra* note 60.

FDA did not take responsibility for the mishandling of the documents.⁷³ 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.⁷⁴

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.⁷⁵ 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.⁷⁶

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

FINDING: 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 processes for the monitoring program caused the FDA to capture protected communications.

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *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.⁷⁷

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.

⁷⁷ 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.⁷⁸

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.**⁷⁹

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.⁸⁰ 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."⁸¹

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.⁸²

⁷⁸ *Id.* at 21 (emphasis added).

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

⁸⁰ *Id.* at 9-10.

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

⁸² 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.⁸³ 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.⁸⁴ As a result, he created an initial document that would govern the investigation.⁸⁵

Laptop Name - DRL0098686

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

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

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

SUBJECT: Robert C. Smith (RCS)
 Medical Officer

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]	DRL0101946 DRL5125449
Cindy Damian	DRL0101600
Nancy Wersto	DRL5114924
Lakshmi Vishnuvajjala	DRL5125617 DRL0096322

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

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

⁸³ Hoofnagle Tr. at 11-12.

⁸⁴ *Id.* at 12.

⁸⁵ 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.⁸⁶

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.⁸⁷

After monitoring two employees' computers, contractors with CNIIT prepared an interim report to describe the status of the surveillance.⁸⁸ 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.⁸⁹

⁸⁶ Hoofnagle Tr. at 25-26.

⁸⁷ See, e.g. Interim Report, *supra* note 10.

⁸⁸ *Id.*

⁸⁹ *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 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.

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

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

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.⁹⁰ 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.

⁹⁰ 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.⁹¹

Dr. Jeffrey Shuren, the highest-ranking FDA employee involved in the monitoring, was equally unaware that the monitoring had captured communications with Congress.⁹² 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?

⁹¹ *Id.*

⁹² 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.⁹³

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."⁹⁴

Dr. Shuren described his concerns about both past leaks and the potential for future leaks.⁹⁵ 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.⁹⁶

Ruth McKee, who acted as a liaison between Dr. Shuren and CNIT, 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

⁹³ *Id.*

⁹⁴ Davis Tr. at 8-11.

⁹⁵ Shuren Tr. at 32-33.

⁹⁶ *Id.*

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

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.⁹⁹ 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.¹⁰⁰

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*.¹⁰¹ Yet, no one conducted an inquiry into past communications.

VIII. Details of the Computer Monitoring

FINDING:	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.”
-----------------	---

⁹⁷ McKee Tr. at 58-60.

⁹⁸ *Id.*

⁹⁹ Newsom Tr. at 34-35.

¹⁰⁰ *Id.*

¹⁰¹ 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.¹⁰² On May 24, 2010, the FDA began monitoring the FDA-issued computer of CDRH scientist Paul Hardy.¹⁰³ On June 30, 2010, the FDA began monitoring the FDA-issued computers of three additional CDRH scientists.¹⁰⁴

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.¹⁰⁵

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.¹⁰⁶ CDRH officials reviewed the information gathered through the monitoring using encrypted flash drives.¹⁰⁷ Information on the encrypted flash drives included private, non-official communications, including Gmail and Yahoo! Mail messages.¹⁰⁸ Transmitted information also contained communications with Congress, confidential attorney-client communications, and confidential complaints filed with the OIG and OSC.¹⁰⁹

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.”¹¹⁰ FDA employees received no notice that this specialized software with such extensive monitoring capability was being installed on their computers.¹¹¹ Moreover, the FDA did not routinely subject all of its employees to such intense scrutiny.¹¹² CNIIT investigator Joseph Hoofnagle, installed the software, and his colleague Christopher Newsom collected the data.¹¹³ 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.¹¹⁴

¹⁰² *Spector Client*, *supra* note 85; Ireland Letter, *supra* note 6.

¹⁰³ See Ireland Letter, *supra* note 6.

¹⁰⁴ *Id.*

¹⁰⁵ Newsom Tr. at 10-11.

¹⁰⁶ *Id.*

¹⁰⁷ McKee Tr. at 13.

¹⁰⁸ See *e.g.*, Newsom Tr. at 54-55.

¹⁰⁹ McKee Tr. at 76.

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

¹¹¹ McKee Tr. at 73.

¹¹² *Id.* at 83.

¹¹³ Newsom Tr. at 8-10.

¹¹⁴ See *e.g.*, Hoofnagle Tr. at 27-28.

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

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?

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

A. To not capture those types of communications is correct.¹¹⁶

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].”¹¹⁷ 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.**¹¹⁸

¹¹⁶ Hoofnagle Tr. at 39.

¹¹⁷ McKee Tr. at 57.

¹¹⁸ *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 Spicree 100, 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 OIG 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.¹¹⁹ 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.¹²⁰ 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.¹²¹

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.¹²² 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

¹¹⁹ Basile Letter, *supra* note 58.

¹²⁰ *Id.* at 2.

¹²¹ McKee Tr. at 29-30.

¹²² 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.¹²³

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.¹²⁴ 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.¹²⁵

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

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

¹²⁴ Albaugh Tr. at 6-8.

¹²⁵ *Id.* at 6-7.

¹²⁶ *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.**¹²⁷

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?

¹²⁷ 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.¹²⁸

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.¹²⁹

* * *

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.¹³⁰

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.¹³¹

¹²⁸ McKee Tr. at 59.

¹²⁹ Davis Tr., at 11.

¹³⁰ *Id.* at 24.

¹³¹ 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.**¹³²

E. Interim Report

Christopher Newsom and Joseph Hoofnagle, CNIIT investigators, drafted an interim report to summarize the status of the surveillance.¹³³ Prior to finalizing the interim report, CNIIT investigators met with FDA managers to review the document.¹³⁴ 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.¹³⁵

¹³² *Id.* at 22 (emphasis added).

¹³³ Hoofnagle Tr. at 34.

¹³⁴ McKee Tr. at 26-27.

¹³⁵ *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.¹³⁶

On June 3, 2010, CNIIT sent the report to Davis and Albaugh.¹³⁷ McKee viewed the report soon after.¹³⁸ 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.¹³⁹

<ul style="list-style-type: none"> • <u>Multiple Gmail contacts with Jack Mitchell (aging.senate.gov) – Emails include attachments with significant amount of documents including those self-redacted.</u> <p style="text-align: center;">View All instances of the above noted in order by date</p>
<ul style="list-style-type: none"> • <u>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.</u> <p style="text-align: center;">View All instances of the above noted in order by date</p>

The interim report also alleged that Dr. Smith "ghostwrote" his subordinates' reports and supplied internal documents and information to external sources.¹⁴⁰ The report confirmed that Dr. Smith spoke with colleagues who shared his concerns about the approval of potentially dangerous products.¹⁴¹ These colleagues also worked with Dr. Smith to shed light on these alleged improprieties.¹⁴² 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.

¹³⁶ Newsom Tr. at 122.

¹³⁷ Interim Report, *supra* note 10.

¹³⁸ McKee Tr. at 26.

¹³⁹ Interim Report, *supra* note 10.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

F. Expansion of People Monitored

Soon after writing the interim report, monitoring was expanded to three additional CDRH employees.¹⁴³ 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.¹⁴⁴

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

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.¹⁴⁶ 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."¹⁴⁷

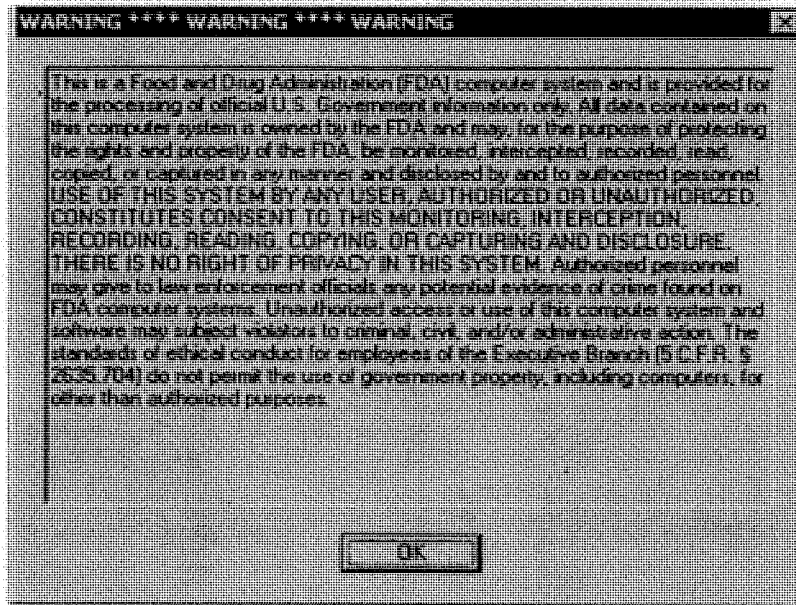
¹⁴³ McKee Tr. at 16.

¹⁴⁴ *Id.* at 57-58.

¹⁴⁵ Newsom Tr. at 122.

¹⁴⁶ Davis Tr. at 54.

¹⁴⁷ *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.¹⁴⁸ She also explained that Joe Albaugh, the FDA Chief Information Security Officer, had the capacity to change the disclaimer language.¹⁴⁹ 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

¹⁴⁸ *Id.* at 53-54.

¹⁴⁹ *Id.*

of Chief Counsel – you have to ask him – on editing this language.¹⁵⁰

Davis later explained that Albaugh changed the disclaimer language because he did not believe the prior language was “tight enough.”¹⁵¹ Although no other FDA Officials interviewed could recall when then change was made, Davis stated that Albaugh decided, to edit the message before monitoring began on CDRH scientists and doctors.¹⁵² 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.¹⁵³

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

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.¹⁵⁵ 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.¹⁵⁶ These personal storage

¹⁵⁰ *Id.*

¹⁵¹ Davis Tr. at 54.

¹⁵² *Id.*

¹⁵³ *Id.* (emphasis added).

¹⁵⁴ Albaugh Tr. at 34.

¹⁵⁵ See Ireland Letter, *supra* note 6.

¹⁵⁶ *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.¹⁵⁷

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.¹⁵⁸ 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."

¹⁵⁷ *Id.*

¹⁵⁸ 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 employees. 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.¹⁵⁹ 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.¹⁶⁰ Dr. Shuren was copied on the e-mail request to the OIG.¹⁶¹ On May 14, 2010, IA wrote to the OIG in response to the allegations contained in GE Healthcare's April 16, 2010, letter.¹⁶² In its response, IA asked the OIG to investigate any disclosure of confidential information by CDRH employees.¹⁶³

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."¹⁶⁴ 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.¹⁶⁵ Later, the OIG clarified the statement to mean that the OIG did not have the authority to determine the legality of such disclosures.¹⁶⁶ Instead, the OIG could refer matters to the Department of Justice if there were "reasonable grounds to believe" there was a criminal law violation.¹⁶⁷ The OIG clarified that the final determination on whether there is potential criminality was the Justice Department's responsibility.¹⁶⁸

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

¹⁵⁹ Shuren Tr. at 14.

¹⁶⁰ Weinstein E-mail, *supra* note 16.

¹⁶¹ *Id.*

¹⁶² 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).

¹⁶³ *Id.*

¹⁶⁴ Vantrease Letter, *supra* note 17.

¹⁶⁵ *Id.*

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

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*

¹⁶⁹ Shuren Letter, June 28, 2010, *supra* note 19.

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

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

On November 3, 2010, the Justice Department wrote to the HHS OIG.¹⁷⁵ The Justice Department explained that the Criminal Division would decline prosecution.¹⁷⁶ 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."¹⁷⁷

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.¹⁷⁸ 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.¹⁷⁹ Dr. Shuren noted that violations of wiretapping laws are felonies, which may subject the person in question to fines and imprisonment.¹⁸⁰ 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.¹⁸¹ Additionally, he expressed concerns over the storage of the recordings, noting the agency's requirements for secured storage and destruction of sensitive information.¹⁸²

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.¹⁸³ Rather, the OIG deferred to the FDA for any necessary administrative action.¹⁸⁴ Still, the monitoring continued according to Dr. Shuren.¹⁸⁵

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?

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ *Id.*

¹⁷⁵ DOJ Letter, *supra* note 21.

¹⁷⁶ *Id.*

¹⁷⁷ Vantrese 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].

¹⁷⁸ Shuren Letter, Feb. 23, 2011, *supra* note 16.

¹⁷⁹ *Id.* at 2.

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² *Id.* at 1-2.

¹⁸³ Inspector Gen. E-mail, *supra* note 177.

¹⁸⁴ *Id.*

¹⁸⁵ Shuren Tr. at 41.

A. Yes.¹⁸⁶

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.**¹⁸⁷

XI. Monitoring Was Not the Solution

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

¹⁸⁶ *Id.*

¹⁸⁷ 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.¹⁸⁸ 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.¹⁸⁹

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.¹⁹⁰

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.¹⁹¹

XII. Managing By Investigation

FINDING:	In spite of 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.

¹⁸⁸ Newsom Tr. at 132.

¹⁸⁹ Shuren Tr. at 93.

¹⁹⁰ Newsom Tr. at 32.

¹⁹¹ 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.¹⁹²

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

¹⁹² 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.**¹⁹³

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.

¹⁹³ *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.¹⁹⁴ 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.¹⁹⁵ Further, the memorandum also purports to safeguard protected communications made using private e-mail accounts.¹⁹⁶ 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."¹⁹⁷ OMB enclosed a memorandum from OSC highlighting that federal law protects whistleblowers' rights.¹⁹⁸

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.¹⁹⁹

¹⁹⁴ 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).

¹⁹⁵ *See id.*

¹⁹⁶ *See id.*

¹⁹⁷ *Id.*

¹⁹⁸ *See id.*

¹⁹⁹ Lerner Memo, *supra* note 24.

OSC addressed the issue of electronic monitoring and protected communications with OSC and OIGs.²⁰⁰ The memorandum failed, however, to acknowledge whistleblowers' rights to communicate with Congress.²⁰¹ OSC issued a press release on February 15, 2012, acknowledging that monitoring employee e-mails should not dissuade employees from making disclosures to Congress.²⁰² 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.”²⁰³ Commissioner Hamburg also directed the CIO and Chief Counsel to “promptly” develop written standards and procedures for monitoring employee personal work computers.²⁰⁴

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.²⁰⁵ 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 Counsel²⁰⁶

²⁰⁰ *Id.*

²⁰¹ *Id.*

²⁰² 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).

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

²⁰⁴ 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).

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

²⁰⁶ *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.²⁰⁷

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.

²⁰⁷ 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.¹

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

¹ 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.

² 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.

CONFIDENTIAL DISCLOSURE – PRIVACY ACT PROTECTED

Appendix I: Relevant Documents

Office of Special Counsel (“OSC”), the Office of Inspector General (“OIG”) and other constitutionally protected communications.³ 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”).⁴ 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.⁵

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).⁶

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)

³ 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 . . .”).

⁴ The Center discovered and located the Logs and Surveillance Cache through a Google search.

⁵ 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.

⁶ 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.⁷ 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.

⁷ 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.⁸ 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.”⁹ These records include, but are not limited to¹⁰:

⁸ 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.

⁹ 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; 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

¹⁰ 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 [REDACTED]” marked “Confidential Attorney-Client Communication”); Bate Stamped No. 1292 (screenshot of inbox email from attorney [REDACTED]” referencing “Office of Special Counsel Filing” with a message stating “Great!”).¹¹

- Documents intercepting confidential communications related to EEO proceedings. See Surveillance Cache, Bate Stamped Nos. 643-684 (emails with Congressional offices about FDA whistleblower [REDACTED]’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 [REDACTED] 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,” [REDACTED] 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 [REDACTED].” Screenshot dated 5/14/10 (page 1340): numerous emails from [REDACTED] 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 [REDACTED] EEO.”

¹¹ 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. 1290.¹²

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

¹² 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.

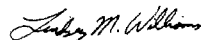
The Surveillance Cache should never have been collected, maintained or distributed.¹³ In particular, interception of OSC, Congressional, and OIG-related records and communications should not be tolerated. Any violations should be subject to the strictest sanction.

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

¹³ 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 M E M O R A N D U M

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 Report¹ entitled "FDA Science and Mission at Risk":

¹ Available at 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.²

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

² 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, █ FDA physicians and scientists █ 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, █ FDA physicians and scientists █ 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] 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.¹ 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



DEPARTMENT OF HEALTH & HUMAN SERVICES

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

Appendix I: Relevant Documents

Page 2 The Honorable Darrell Issa

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.

Page 3 – The Honorable Darrell Issa

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

Page 4 – The Honorable Darrell Issa

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.

- ██████████ 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, ██████████ has been temporarily reappointed with pay through July 31, 2012.
- ██████████ 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).
- ██████████ 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.
- ██████████ 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.¹

¹ 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.

Page 7 – The Honorable Darrell Issa

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,



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: Lon 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

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

View All instances of the above noted in order by date

- o 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

- o RCS and JN are in communication with Kahn regarding articles

View All instances of the above noted in order by date

- o 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

202

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

Received

January 13, 2009

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

www.hhlaw.com

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

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

07/4/2009 1:57 PM

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 (TS) 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.

4/24 1:57 PM

 NYT Jan 13
2009.pdf (36 KB)

 [redacted] -- 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, [redacted] 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 [redacted] who now has the lead for the overall investigation into the allegations from the Radiological Devices Branch, and [redacted] 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 [redacted]
10903 NH Ave.
Silver Spring MD 20993
[redacted]



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 #: H10#001413

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 (OLA 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 & 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

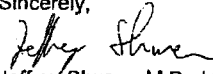
application files. In the case of the FFDM device submission, the employees sharing and discussing the company-confidential information with the unauthorized recipient were officially assigned to review these files, but the unauthorized recipient lacked any prior history with these files or specific 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,

A handwritten signature in black ink, appearing to read "J. Smith".

Jack Smith
Chief
Public Integrity Section

P2
P1

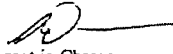


DEPARTMENT OF HEALTH AND HUMAN SERVICES

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

NOV 16 2010


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

FROM: Scott A. Vantrese 
 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. Vantrese at .

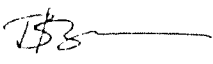


EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 20, 2012

MEMORANDUM FOR CHIEF INFORMATION OFFICERS AND GENERAL COUNSELS

FROM: Steven VanRoekel 
Federal Chief Information Officer

Boris Bershteyn 
General Counsel

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 authorities¹ and are expected to maintain concern for the public interest,² 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.³ Subject to certain exceptions, Federal law also protects the identity of an employee who makes

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

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

³ 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).⁴

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.

⁴ 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]

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.



 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.”¹ 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 Report² 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.³ This letter also provides elements of reform that are necessary to begin real change at FDA from the “bottom up.”

Since May 2008,⁴ 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 requires⁵ that safety and effectiveness is determined based on “valid scientific evidence ... from which it can fairly and responsibly be

Page 2 of 6 – Mr. Podesta

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,⁶ are not publicly available, and, if followed, would circumvent science and legal regulatory requirements;
- Fail to properly document significant decisions in the administrative files;⁷
- 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 Meetings⁸ 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.⁹ The failure of Dr. von Eschenbach and Mr. McConagha to take appropriate or effective actions has made them complicit in the wrongdoing,¹⁰ 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, 2008,¹¹ 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

Page 3 of 6 – Mr. Podesta

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*¹² 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,¹³ 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) devices¹⁴ 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 detection¹⁵ and they were associated with increased patient recalls and unnecessary breast biopsies.¹⁶ 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.¹⁷ 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.¹⁸ 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

Page 4 of 6 – Mr. Podesta

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 2008¹⁹ 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 President²⁰ sign, new legislation providing the strongest possible protections for all government employees,²¹ 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.²² “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 Policy²³ 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

Page 5 of 6 – Mr. Podesta

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.”²⁴ 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 Stupak²⁵ 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.²⁶ FDA must not engage in a fire-fighting regulatory posture after medical products are introduced into clinical practice and used on patients.²⁷ 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.²⁸ This will provide FDA with the necessary critical scientific capability and capacity²⁹ 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.³⁰ 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,

Page 6 of 6 – Mr. Podesta

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

- ¹ See <http://change.gov/agenda/>
- ² See http://www.fda.gov/ohrms/dockets/ac/07/briefing/2007-4329b_02_00_index.html
- ³ 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>
- ⁴ 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.
- ⁵ See 21 CFR 860.7.
- ⁶ See 21 CFR 10.115.
- ⁷ See 21 CFR 10.70.
- ⁸ See <http://www.citizen.org/publications/release.cfm?ID=7620>
- ⁹ See letter to Mr. Bill McConagha dated October 20, 2008.
- ¹⁰ See letter to Dr. Andrew von Eschenbach dated September 29, 2008.
- ¹¹ See <http://energycommerce.house.gov/images/stories/Documents/PDF/Newsroom/110-ltr-111708.vonEschenbach.CDRH.pdf>
- ¹² EEOC No. 531-2006-00114X.
- ¹³ 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.
- ¹⁴ *Id.* at page 121.
- ¹⁵ See <http://www.fda.gov/ohrms/dockets/ac/08/briefing/2008-4349b1-01%20FDA%20Radiological%20Devices%20Panel%20Meeting%20Introduct.pdf> at pages 52-56.
- ¹⁶ See *Id.* at pages 42 and 52-56.
- ¹⁷ See 21 CFR 860.7.
- ¹⁸ See <http://www.fda.gov/CDRH/MAMMOGRAPHY/scorecard-statistics.html>
- ¹⁹ See <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfAdvisory/details.cfm?mtg=694>
- ²⁰ See http://www.whistleblowers.org/index.php?option=com_content&task=view&id=695&Itemid=100
- ²¹ 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.
- ²² See http://change.gov/agenda/ethics_agenda/
- ²³ See http://change.gov/page/-/open%20government/yourseatatthetable/SeatAtTheTable_memo.pdf
- ²⁴ See http://change.gov/agenda/ethics_agenda/
- ²⁵ See <http://online.wsj.com/public/resources/documents/stupak-letter-to-obama-20081205.pdf>
- ²⁶ See <http://www.fda.gov/cdrh/strategic/tplc.html>
- ²⁷ 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
- ²⁸ See <http://www.hhs.gov/about/orgchart/>
- ²⁹ 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
- ³⁰ 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/hus/07.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.

Appendix I: Relevant Documents

Newer and looking



January 13, 2009

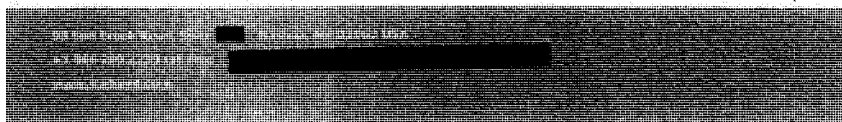
Les S. Weinstein
 Ombudsman and Quality Assurance Manager
 Center for Devices and Radiological Health (HFZ-5)
 Food and Drug Administration
 9200 Corporate Boulevard
 Rockville, Maryland 20850

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®.



Appendix I: Relevant Documents

Hever, Inc.



On Friday, January 9, I personally spoke with Mr. Harris by phone with Ms. Darlene Deputa-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,

Ken Ferry
President and Chief Executive Officer

Cc: [REDACTED], M.D.
[REDACTED], Ph.D.
[REDACTED], M.D., J.D.



KING & SPALDING LLP

King & Spalding LLP
1700 Pennsylvania Avenue, N.W.
Washington, DC 20006-4704Edward 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
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_MANAGE-145966.1

April 16, 2010

Page 2

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 pre-market 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

WDC_IMANAGE-1455055.1

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-1445061

April 16, 2010
Page 4

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)

WDC_IMANAGE-145003.1

April 16, 2010
Page 5

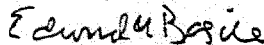
submissions. FDA may only disclose the existence of a 510(k) submission for a device that is not on the market and where the intent to market the device is not public if the submitter has not designated the submission as confidential or made the proper certifications, or FDA disagrees with the designation. 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-1455065 1



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

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

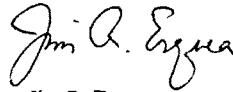
were highly sensitive and requested that the copying job be assigned a contractor that had prior experience with large copying jobs of sensitive and confidential documents. The PSC designated QAI under a Simplified Purchase Agreement (SPA), a streamlined printing procurement vehicle used by the GPO's 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 16th (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



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 3rd. 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 9th. Our records show that the files were archived on May 9th.

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
Paul Swidersky
President, CEO


90 Invoice Documents

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

DEPARTMENT DH-HSPDIA		REQ. NO. 2-08004-	JACKET NO. 372-828	RFA NO. 980	WORK ORDER NO. 89308
CLASSIFICATION Classified <input type="checkbox"/> Unclassified <input checked="" type="checkbox"/> SBU <input type="checkbox"/> FPI <input type="checkbox"/> FPO <input type="checkbox"/>		PUBLICATION TITLE LITIGATION FILE ORGANIZATION		DATE PREPARED 05/23/2012	OBJECT CLASS
CONTRACTOR Query Associates Inc		PURCHASE ORDER NO. 80845	STATE CODE 180	CONTRACTOR'S CODE 72508	SHIP/DELIVERY DATE 5/25/2012
NOT FOR CONTRACTOR USE	BILLING ADDRESS CODE (BAC) 4164-01	AGENCY LOCATION CODE (ALC) 7500088	APPROPRIATION CHANGEABLE/OBLIGATION NO. 89999VC		
	Pay by <input type="checkbox"/> Purchase Card <input checked="" type="checkbox"/> Card		PURCHASE CARD NO. (only to appear on GPO Copy Only) EXP. DATE NAME AS IT APPEARS ON PURCHASE CARD		
	PHONE NO. OF CARDHOLDER		EMAIL OF PURCHASE CARDHOLDER		TREASURY ACCOUNT SYMBOL (TAS)
	LINE OF ACCOUNTING REFERENCE NUMBER (only will appear on IFAC as Entered) 2000081				
SPECIFICATIONS	PROOFS <input type="checkbox"/> Contact <input type="checkbox"/> Email <input type="checkbox"/> High Resolution <input type="checkbox"/> Prior to Production Samples <input type="checkbox"/> Electronic <input type="checkbox"/> Soft Proof		DAYS DEPT. WILL HOLD PROOFS	QUALITY LEVEL	QUANTITY
	PUBLISHED ELECTRONIC MEDIA <input type="checkbox"/> Files to be sent via FTP or Email <input type="checkbox"/> CD/DVD		OTHER BOUY. PUBLISHED MATERIALS		PRINTS SHEET INSPECTION <input type="checkbox"/> No. of Home Marks
	COVER PAPER	COLOR OF COVER INKS	COVER COATING TYPE	PAPER COVERS (Sheet) (Separate)	INDICATE WHICH COVERS PRINT 1 2 3 4
	TEXT PAPER	COLOR OF TEXT INK	TEXT COATING TYPE	NUMBER OF TEXT PAGES	PRINT <input type="checkbox"/> One Side <input type="checkbox"/> Head to Head <input type="checkbox"/> Head to Tail
ADDITIONAL INFORMATION	BIBLIO <input type="checkbox"/> ULD <input type="checkbox"/> BND <input type="checkbox"/> SADDLE <input type="checkbox"/> COMB <input type="checkbox"/> COV. <input type="checkbox"/> PERFECT BOUND <input type="checkbox"/> BSW <input type="checkbox"/> TAPE <input type="checkbox"/> TRIM 4 SIDES <input type="checkbox"/> OTHER				
	Description Organize and label number 89,888 files. Create pdf's and email to address supplied. Please send email to [redacted] when job is delivered. DPA, Megan, Shannon to JAMES MELTON, 8880 Fishers Lane, Parkersburg W. Va. [redacted] Beckwith, MD 20827 *Delivery hours for the Purchase Order are 8:00 am to 12:00 pm - 1:00 pm to 4:00 pm. Deliveries must be made by the [redacted] date.* All business are [redacted] to U.S. Government Printing Office, Office of the Comptroller, STOP FACA, Washington, DC 20541 or [redacted] to [redacted] include program and work no. on orders to insure proper payment.				
	DELIVER PRODUCT TO: RETURN PUBLISHED MATERIAL TO:				
	<input type="checkbox"/> Classification List Attached Digital Deliverables Requested - Format: <input type="checkbox"/> Native <input type="checkbox"/> PDF				
SUPT. DOCS. NOTIFIED <input checked="" type="checkbox"/> Yes <input 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.	
AUTHORIZED SIGNATURE (must be on file with GPO)		DATE SENT TO CONTRACTOR 5/23/2012		DATE ORDER RECEIVED 5/23/2012	
ORDER RECEIVED BY: (Agency Representative)		CONTRACTOR SIGNATURE		DATE	

Web Estimate - May 2012



Quality Associates, Inc.
 8181 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
PBC Contact: [REDACTED]
Project: Conversion Services
Agency: PSC - Div of Support Services
PSC Contact Phone: 301-[REDACTED]
Email: [REDACTED]
Prepared By Name: [REDACTED]
Phone: [REDACTED]

1	Analyze data from client supplied hard drive. Convert files from various formats to pdf for printing	1	\$4,000.00	\$4,000.00
			SUBTOTAL:	\$ 4,000.00

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
W066 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 external, 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 black ink, which appears to read "Mark S. McCormack".

Mark S. McCormack
Special Agent in Charge

Enclosure

Cc:
Case File
Chron



Food and Drug Administration
Office of Internal Affairs

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: SAJC 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. McGuire* 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,

A handwritten signature in black ink, appearing to read "SAV", followed by a horizontal line.

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]



DEPARTMENT OF HEALTH & HUMAN SERVICES

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

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.

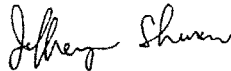
The employees seem to have been in several different physical locations, all of which were likely in the State of Maryland, when they made the recordings. In particular, the recordings suggest that they were variously recording the calls and meetings from their FDA offices (in White Oak, Maryland or 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.¹ 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...."² Violations are felonies subject to imprisonment and fines.³ Federal law appears to require the consent of only one party to the interception of a phone call,⁴ 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

¹ 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.

² Md. COURTS & JUDICIAL PROCEEDINGS Code Ann. § 10-402(c)(3) (emphasis added). Other exceptions apply, which do not appear to be relevant here.

³ *Id.* § 10-402(b).

⁴ See 18 U.S.C. § 2511.

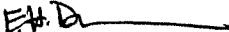


DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the General Counsel

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 

RE: Requirements 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.¹ 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.²

Pursuant to this memorandum, which is effective immediately, I am directing that the CIO and Chief Counsel³ 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.

¹ 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 delegatee.

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.

² 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.

³ FDA's Office of the Chief Counsel is part of HHS' Office of General Counsel (OGC); I expect that in advising FDA, OGC 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.⁴

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

⁴ 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.



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration
Silver Spring MD 20993

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

Appendix I: Relevant Documents

Page 2

(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)*,¹ 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,² (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

¹ Available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>

² 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."

Page 3

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

Page 4

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.

Page 5

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))³ 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 (OSSSI) 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,

³ For the purposes of this interim policy, the term "law enforcement authority" includes national security and intelligence agencies of the U.S. Government.

Page 6

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

Page 7

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

Page 8

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.

Page 9

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.



Date: 9/26/13

Walter S. Harris, MBA, PMP
Deputy Commissioner for Operations
Chief Operating Officer

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

DAN BURTON, INDIANA
JOHN L. COCA, FLORIDA
TODD RUSSELL PLATTS, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
PATRICK ROBERTY, NORTH CAROLINA
JIM JOHNSON, OHIO
JABON COMBETZ, OREGON
CONNIE MACK, FLORIDA
TOM MALBERG, MICHIGAN
JAMES LANKFORD, OREGON
JUSTIN AMASH, MICHIGAN
JOE BARTY, NEW YORK
PAUL A. GOSAR, ARIZONA
RICK L. LARABEE, ALABAMA
PATRICK ROBERTY, PENNSYLVANIA
BOBBY L. RICHARDS, TENNESSEE
JOE WALSH, ILLINOIS
TREV GONDOY, SOUTH CAROLINA
DENNIS A. ROSS, FLORIDA
FRANK C. LUONGO, NEW HAMPSHIRE
BLAKE FARENTHOLD, TEXAS
BRUCE MCELROY, MISSOURI
LAWRENCE J. BRADY
STAFF DIRECTOR

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

MASSPH (202) 225-5076
FACSIMILE (202) 225-5074
TELEPHONE (202) 225-5000
<http://www.migpl.house.gov>

May 9, 2012

ELIJAH B. CUMMINGS, MARYLAND
RANKING MEMBER

EDOLPHUS TOWNS, NEW YORK
CAROLYN B. MALONEY, NEW YORK
CLEOPHOLMES MORTON,
DISTRICT OF COLUMBIA
DENNIS S. KUCINICH, OHIO
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNN, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
MIKE DUGLEY, ILLINOIS
DAN R. BURKE, ILLINOIS
BRUCE L. BRALEY, IOWA
PETER WELLS, CONNECTICUT
JOHN A. YARMOUTH, KENTUCKY
CHRISTOPHER S. MURPHY, CONNECTICUT
JACKIE SPEER, CALIFORNIA

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.¹ 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.² 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.³ Instead, under POLA's proposal, only trucking companies utilizing employee-drivers, who are subject to unionization, would be allowed to work at the

¹ THE BEST PLACES TO WORK IN THE FEDERAL GOVERNMENT (2011), <http://bestplacestowork.org/BPTW/rankings/overall/small>.

² Ronald D. White, *Agency Objects to Clean Truck Program*, L.A. TIMES, Oct. 30, 2008.

³ S. Calif. Port Truck Plan Supporters Warn Current Version Will Fail, SHIPPERS' NEWSWIRE, July 5, 2007.

The Honorable Richard A. Lidinsky, Jr.
 May 9, 2012
 Page 2

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.”⁴

Labor unions,⁵ environmental groups,⁶ 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.⁷ 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.⁸ 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

⁴ 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).

⁵ 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>.

⁶ David Pettit, *A Truckload of Hypocrisy*, NATURAL RESOURCES DEFENSE COUNCIL, Sept. 17, 2008, http://switchboard.nrdc.org/blogs/dpetit/a_truckload_of_hypocrisy.html.

⁷ 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/>.

⁸ 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).

The Honorable Richard A. Lidinsky, Jr.
 May 9, 2012
 Page 3

performance time? I will decide in the future what time he has. Take this up with his supervisor, RL.⁹

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.¹⁰ According to documents reviewed by the Committee, this would have equated to awards of roughly \$3,800 to \$4,200, respectively.¹¹

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."¹² 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.¹³

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."¹⁴ 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.¹⁵ 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.

⁹ E-mail from Richard A. Lidinsky, Chairman, Federal Maritime Commission, to Ronald Murphy, Managing Director, Federal Maritime Commission (July 14, 2011).

¹⁰ FEDERAL MARITIME COMMISSION, RECOMMENDATION FOR PERFORMANCE OR INCENTIVE AWARD (Sept. 20, 2010).

¹¹ FEDERAL MARITIME COMMISSION, *supra* note 10.

¹² Memoranda from Rebecca Dye, Commissioner, Federal Maritime Commission to Austin Schmitt, Director, Bureau of Trade Analysis (Sept. 13, 2010) (on file with author).

¹³ FEDERAL MARITIME COMMISSION, *supra* note 11, § (f)(7).

¹⁴ Memorandum from Ronald D. Murphy, Managing Director, Federal Maritime Commission to Austin Schmitt, Director, Bureau of Trade Analysis (Sept. 22, 2010).

¹⁵ SpectorSoft, Computer & Internet Monitoring Software, <http://www.spector360.com/> (last visited May 8, 2012).

The Honorable Richard A. Lidinsky, Jr.
 May 9, 2012
 Page 4

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.

The Honorable Richard A. Lidinsky, Jr.
May 9, 2012
Page 5

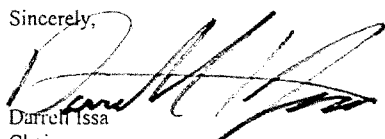
4. A complete accounting of the agency's procurement of a vehicle for the purpose of transporting commissioners and agency employees, including:
 - a. The year, make and model of the vehicle;
 - b. The total amount spent on the vehicle, including any costs involved in securing garage space for the vehicle;
 - 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,


Durrah Issa
Chairman

Attachment

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Appendix I: Relevant Documents

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ELIJAH E. CUMMINGS, MARYLAND
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.

1

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.

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM COCHRAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. COSAB, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAYS, TENNESSEE
THEY GOUDY, SOUTH CAROLINA
ELINE FARENTHOLD, TEXAS
GOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
BOB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KEVIN I. BERTHOUD, MICHIGAN
RON DISANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH 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

Facsimile (202) 225-3874

Minority (202) 225-5051

<http://oversight.house.gov>

February 25, 2014

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN E. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
MARK POCAN, WISCONSIN
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY GARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Ranking Member Cummings:

I received your letter requesting a postponement of the February 26, 2014, full Committee hearing entitled "Limitless Surveillance by the FDA: Protecting the Rights of Federal Whistleblowers."¹ I am surprised by your efforts to thwart a hearing exposing unprecedented computer monitoring of employees at the Food and Drug Administration, especially when it became clear that FDA officials approved this monitoring without regard for the employees' right to communicate with Congress.

During this joint investigation with Senator Grassley, the Committee conducted transcribed interviews in which your staff participated fully. Senator Grassley's Democratic counterparts were also invited to participate, but they declined. Your request to postpone appears to be yet another attempt to obstruct the progress of the Committee as it seeks to expose waste, fraud, abuse and mismanagement in our federal government.

In fact, the reasons from the FDA and your office for requesting a postponement for the hearing have shifted several times in less than a week. First, the FDA told the Committee that its witnesses needed more time to prepare, despite having known about this hearing since January 14, 2014. Next, the FDA stated that scheduling conflicts would prevent their witnesses from testifying. Then, your staff requested a postponement to allow the HHS Inspector General additional time to complete its report on the FDA monitoring. Now, according to your letter, your staff needs additional time to interview the whistleblowers. In fact, as your staff knows, the FDA whistleblowers expressed serious reservations about providing documents and information to your staff, based on a belief that you and your staff work hand in hand with the federal agencies under investigation by the Committee. Based on the events of the past week—in which I have heard requests to postpone the hearing from FDA, your staff, and now you—it is obvious why they would think that.

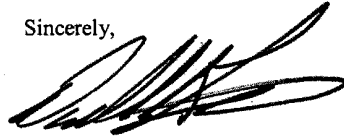
¹ Letter from Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight and Gov't Reform, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight and Gov't Reform (Feb. 24, 2014).

The Honorable Elijah E. Cummings
February 25, 2014
Page 2

I am also concerned that you and your staff—perhaps unwittingly—partnered with the FDA in an attempt to mislead the Committee. On February 20, 2014, your staff wrote an e-mail to my staff—based on one of many conversations your staff had with Administration officials that excluded the Majority staff—claiming that FDA “informed us that the IG has already completed a draft report, that the FDA has already submitted its comments to the draft report, and that they expect the final report to be released ‘imminently.’”² In fact, FDA did not submit its comments to the draft until the next day, February 21, 2014.³

Throughout this investigation, your staff focused on the conduct of the whistleblowers that were under surveillance, as part of an apparent effort to justify the actions of the FDA. Despite your often hostile posture towards federal employee whistleblowers who contact Congress about waste, fraud, abuse and mismanagement at federal agencies, I will continue to position this Committee as a safe place where whistleblowers can confidently bring their allegations. In the future, I hope you will work with me to safeguard protected communications with Congress instead of attempting to obstruct a hearing aimed at exposing mismanagement and supporting the rights of whistleblowers.

Sincerely,



Darrell Issa
Chairman

² E-mail from H. Comm. on Oversight & Gov't Reform Minority Staff to H. Comm. on Oversight & Gov't Reform Majority Staff (Feb. 20, 2014, 3:17 p.m.). (emphasis added)

³ Telephone call with HHS OIG staff (Feb. 21, 2014).