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

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) submission[3] 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 1after 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 employees[20] 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

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:

1. 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 webpage[1] and the Office of the Chief Information Officer (OCIO) webpage[2]. 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/ohr/whistleblower.html
[2] http://intranet.hhs.gov/it/cybersecurity/policies/index.html

1

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.