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 prison[2] 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/ICECI/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 2002[8] 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-partI-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-subchapIII-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 Monitoring[16]

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 Behavior[19] 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 2012[25] (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.