1. PURPOSE.

This Staff Manual Guide establishes interim policies and procedures that will strengthen the Food and Drug Administration’s (FDA) ability to effectively document, analyze, authorize, and manage requests to monitor use of Department of Health and Human Services (HHS or Department) and FDA information technology (IT) systems and resources.

2. SCOPE.

This interim policy:

- Applies to all individuals (including, but not limited to current and former civilian government employees, contractors, local or foreign government exchange program participants, Commissioned Corps personnel, guest researchers, visiting scientists, fellows and interns), provided access to HHS/FDA IT systems and resources;
- Covers real-time or contemporaneous observation, prospective monitoring (e.g., using monitoring or keystroke capture software), and retrospective review and analyses (e.g., of e-mail sent or received, or of computer hard-drive contents) targeting an individual;
- Does not apply to computer incident response monitoring of systems relating to national security or the Federal Information Security Management Act of 2002 (FISMA) that perform general system and network monitoring, or examinations of computers for malware;
- Does not apply to any review and analysis requested or consented to by the individual(s) being monitored;
- Does not apply to retrospective searches for documents in response to valid information requests in the context of litigation, Congressional oversight, Freedom of Information Act
(FOIA) requests, and investigations by the Government Accountability Office (GAO) and the Office of Special Counsel;

- This interim policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in place as of this interim policy’s effective date; and

- Excludes routine IT equipment examinations. Any unintended discoveries of problematic content and resulting follow-up actions are not subject to this interim policy, although follow-up actions that involve computer monitoring are subject to this interim policy.

3. BACKGROUND.

FDA is required to protect vast quantities of sensitive information including, but not limited to, confidential commercial and financial information, trade secrets, protected healthcare information, and classified information. The Department of Health and Human Services (HHS) Policy for Information Systems Security and Privacy (IS2P),¹ requires the use of a warning banner on all Department IT systems. The warning banner must state that, by accessing an HHS/FDA IT system,² (e.g., logging onto a Department computer or network), the employee consents to having no reasonable expectation of privacy regarding any communication or data transiting or stored on any HHS/FDA IT system, and the employee understands that, at any time, the Department may monitor the use of Agency IT resources for lawful government purposes. While the warning banner gives FDA the authority to monitor employee use of Agency IT resources, FDA must carry out computer monitoring in a manner that recognizes employee interests and relevant legal protections. FDA will comply with all applicable laws, including but not limited to the Privacy Act of 1974, the privacy provisions of the E-Government Act of 2002, Whistleblower Protection Enhancement Act of 2012, and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts.

4. REFERENCES.

HHS Policy for Monitoring Employee Use of HHS IT Resources, dated June 26, 2013
FDA Memorandum, Monitoring of FDA Personnel Work Computers, dated September 24, 2012
HHS IRM Policy for Personal Use of Information Technology Resources dated February 17, 2006
HHS Policy for Information Systems Security and Privacy, dated July 7, 2011
NIST SP 800-61, Computer Security Incident Handling Guide, dated March 2008
NIST SP 800-86, Guide to Integrating Forensic Techniques - Incident Response, August 2006

¹ Available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html

² According to the warning banner, an HHS IT system includes "(1) the computer being accessed, (2) the computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network."

5. INTERIM POLICY.

5.1. BASIS FOR COMPUTER MONITORING.

Computer monitoring may be authorized only for the following reasons:

a. A written request by OIG, OSS or an outside law enforcement authority (e.g., FBI, DHS);
b. Where reasonable grounds exist to believe that the individual to be monitored may be responsible for the unauthorized disclosure of legally protected information (e.g., confidential commercial information or Privacy Act-protected information); or
c. Where reasonable grounds exist to believe that the individual to be monitored may have violated applicable law, regulation or written HHS or FDA policy.

5.2 EXPRESS WRITTEN AUTHORIZATION FOR COMPUTER MONITORING.

No agency official, including the Chief Information Officer (CIO), may conduct computer monitoring without prior written authorization by one of the following officials:

- FDA Commissioner
- FDA Deputy Commissioner
- FDA Chief Operating Officer

The authority identified herein may not be (re)delegated below the office of Chief Operating Officer. All requests to initiate monitoring must be in writing and shall include an explanation of how the monitoring will be conducted, by what method the information collected during monitoring will be controlled and protected, and a listing of individuals who will be provided access to the information gathered through monitoring. Except for monitoring requested by outside law enforcement authority or the OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. The requesting organization shall document the basis for any request for computer monitoring.

5.3 REVIEW COMMITTEE.

A Review Committee shall be established as described below and as further set forth in implementing procedures. This Review Committee shall consist of a representative from the Office of the Chief Counsel, a representative from the Office of Information Management with Systems Administration expertise, and a representative from the Office of Human Resources
with Human Capital expertise. The Review Committee may draw on additional expertise, as needed.

For designated requests for monitoring, the Review Committee shall review such requests and recommend to an authorizing official specified in 5.2 above, that the official authorize or not authorize a specific request. For other requests, the Review Committee will not ordinarily recommend authorization or non-authorization, although it may at its discretion put a request on hold or make a recommendation concerning authorization to an FDA authorizing official as specified in 5.2 above.

The Review Committee shall develop, as soon as practicable, procedures by which it will review and receive notification of requests for computer monitoring and, if appropriate, explain how such requests are to be submitted and documented. The Review Committee’s procedures should ensure that the Committee promptly and efficiently reviews requests for computer monitoring that require a Committee recommendation to an agency authorizing official or which require that the Review Committee be notified of such requests.

In developing implementing procedures, the Review Committee should consider the following framework for review, authorization, and notification of requests for computer monitoring:

a. Requests from outside law enforcement: The Review Committee should be notified of requests from outside law enforcement for which a Memorandum of Understanding (MOU) or similar written agreement is in effect. Provided such an MOU or similar written agreement is in effect (see 5.4 below), the Review Committee will not ordinarily make a recommendation concerning such requests to an FDA authorizing official. If an MOU or similar written agreement is not in effect, all such requests should be provided to the Review Committee for review and recommendation.

b. Requests from OIG: The Review Committee should be notified of requests from OIG.

c. Requests from sources other than outside law enforcement/OIG for prospective monitoring should be provided to the Review Committee for review and recommendation to an authorizing official.

d. Requests from sources other than outside law enforcement/OIG for retrospective monitoring should, when implementing procedures have been developed, be provided to the Review Committee for review and recommendation, or notification and appropriate action.
5.4 MONITORING REQUESTS FROM OIG AND OUTSIDE LAW ENFORCEMENT.

Computer monitoring may be requested by outside law enforcement authorities (e.g., Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS))\(^3\) or the HHS Office of Inspector General (OIG). All requests from outside law enforcement agencies must be coordinated through the OIG, except for requests relating to national security or non-criminal insider threat matters, which must be coordinated with the Office of Security and Strategic Information (OSSI) and/or the FDA Security Liaison Officer/Insider Threat Coordinator. Such external computer monitoring requests may be subject to different standards partly because they are covered by the internal controls of the requesting agency or judicial process.

If the monitoring is requested by outside law enforcement authorities, a Memorandum of Understanding (MOU) or similar written agreement may be developed with outside law enforcement as a precondition for approving computer monitoring requests from these organizations.

Such an MOU or similar written agreement shall include the following:

a. The title and organizational component of the person(s) authorized to request monitoring on behalf of the law enforcement agency;
b. Documentation of the source of the official request, demonstrating approval by an official of the governmental entity that has the authority to request the initiation of such monitoring (e.g., a subpoena (administrative or grand jury)), warrant or national security letter (NSL), or other acceptable documented request (e.g., a written administrative request that meets the HIPAA Privacy Rule’s requirements for certain disclosures to law enforcement agencies);
c. Any restrictions applicable to the handling and disclosure of confidential information that may be produced by the computer monitoring; and
d. Other items consistent with this memorandum, including the handling of sensitive communications.

5.5 SCOPE OF COMPUTER MONITORING.

Requests for computer monitoring shall be narrowly tailored in time, scope, and degree of monitoring. All requests to monitor shall identify the least invasive approach to accomplish the monitoring objectives. When reviewing requests for monitoring, authorizing officials shall also consider whether there are alternative information-gathering methods available (in lieu of monitoring) that can be utilized to address the potential risk, without jeopardizing the agency’s objectives. When the monitoring request originates from OIG or outside law enforcement,

\(^3\) For the purposes of this interim policy, the term “law enforcement authority” includes national security and intelligence agencies of the U.S. Government.
the authorizing official will grant appropriate deference to requests made in accordance with this memorandum.

5.6 DOCUMENTATION.

The written authorization for computer monitoring must describe the reason for the monitoring. If the monitoring is initiated at the request of outside law enforcement, the authorization must document that the request was approved by an official of the governmental entity that has the authority to request the initiation of such monitoring.

Except for computer monitoring initiated at the request of an outside law enforcement authority or OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. Requests for such monitoring must include: an explanation of how the monitoring will be conducted, by what means the information collected during monitoring will be controlled and protected, and, a listing of individuals who will be provided access to the resultant monitoring information.

A record of all requests for monitoring shall be maintained by the FDA COO, along with any other summary results or documentation produced during the period of monitoring. The record also shall reflect the scope of the monitoring. All information collected from monitoring and maintained by the FDA COO must be controlled and protected, with distribution limited to the individuals identified in the request for monitoring and other individuals specifically designated by the COO as having a specific need to know such information.

5.7. LIMITING THE TIME, SCOPE AND INVASIVENESS OF MONITORING.

The FDA COO will authorize computer monitoring that is appropriately narrow in scope, time-limited, and takes the least invasive approach to accomplish monitoring objectives. The COO, in reviewing requests for computer monitoring, must also consider whether there are alternative information-gathering methods that FDA can utilize to address the concern in lieu of monitoring. When the computer monitoring request originates from OIG or outside law enforcement, the COO authorizing the monitoring will grant appropriate deference to a request made in accordance with this interim policy.

5.8. SENSITIVE COMMUNICATIONS.

No computer monitoring authorized or conducted may target communications with law enforcement entities, the Office of Special Counsel, members of Congress or their staff, employee union officials, or private attorneys. If such communications are inadvertently collected or inadvertently identified from more general searches, they may not be shared with a
non-law enforcement party who requested the monitoring, or anyone else, without express written authorization from OGC and other appropriate HHS and FDA official(s).

5.9. PERIODIC REVIEW OF MONITORING.

The COO shall review all computer monitoring on a monthly basis and, in consultation with the party who requested the monitoring (e.g., OCI), assess whether it remains justified or must be discontinued. The COO shall consider if the decision for ongoing computer monitoring should be reviewed by OGC. A decision to continue monitoring shall be documented in writing by the COO, who shall report at least monthly, to the Commissioner regarding the status of any ongoing monitoring.

5.10. LEGAL REVIEW.

Review by the FDA Office of the Chief Counsel of a request for computer monitoring will include, as necessary, consultation with other Divisions of HHS Office of the General Counsel, such as the General Law Division, especially concerning legal requirements such as the Whistleblower Protection Act and the HIPAA Privacy and Security Rule, about which other OGC Divisions have expertise.

5.11 SPECIAL CIRCUMSTANCES.

The authorizing official and Chief Counsel may make recommendations to the Commissioner for additional procedures, if necessary, to address specific circumstances not addressed in this Staff Manual Guide. Policies and procedures that deviate from the elements of the HHS Memorandum may not be implemented without the written concurrence of the HHS COO in consultation with the OGC.

6. ROLES AND RESPONSIBILITIES.

FDA Chief Counsel. Provides legal review and advice regarding requests for, and implementation of, computer monitoring of HHS IT systems and resources. OCC will consult with HHS OGC as needed.

FDA Chief Operating Officer (COO). The COO Provides executive direction, leadership, coordination, and guidance for the overall day-to-day administrative operations of the FDA ensuring the timely and effective implementation and high quality delivery of services across the Food and Drug Administration (FDA). The COO will coordinate with the Office of Chief Counsel, the Chief Information Officer, Office of Criminal Investigation (OCI), law enforcement and other authorities on actions and activities involving monitoring of use of IT Resources.

FDA Chief Information Officer (CIO). The CIO in the Office of Information Management (OIM) is responsible for executing monitoring as authorized by the Commissioner and COO
following consultation with Chief Counsel. The CIO provides the overall policy, guidance and general oversight of FDA’s electronic records and for establishing and implementing the agency incident response plan for responding to the detection of adverse events involving FDA information systems.

**FDA Chief Information Security Officer (CISO).** The FDA CISO is responsible for the establishment and management of the FDA incident response process. The FDA CISO serves as an FDA focal point for incident reporting and subsequent resolution. The CISO provides advice and assistance to Agency managers and other organizational personnel concerning incident response activities.

**FDA Computer Security Incident Response Team (CSIRT).** Headed by the CSIRT Lead, the Incident Response (IR) Team will conduct computing monitoring, forensic capabilities and techniques in accordance with established NIST Standards. The CSIRT provides centralized monitoring, tracking, analysis, insider threat detection, reporting, notification, and coordination of computer security incidents and to report the finding with the appropriate officials in support of law enforcement and national security officials.

### 7. DEFINITIONS.

**Employee** - All individuals (e.g., including, but not limited to current and former civilian government employees, contactors, local or foreign government exchange program participants, Commissioned Corp personnel, guest researchers, visiting scientists, fellows and interns), provided access to Department of Health and Human Services, Food and Drug Administration IT systems and resources.

**IT System** - Includes (1) the computer or electronic device being accessed, (2) the computer network (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.

**Accessing an HHS/FDA System** - e.g., logging on to a government or contractor furnished computer, laptop, Blackberry, iPad, scanner or other electronic device or logging on to the FDA network via local or remote use.

**IT Resources** - Includes but is not limited to: computers and related peripheral equipment and software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to internet services, e-mail and, for the purposes of this policy, office supplies. It includes data stored in or transported by such resources for HHS/FDA purposes.

**Outside Law Enforcement Authority** - Includes national security and intelligence agencies of the United States.
Passive Monitoring/Computer Incident Response Monitoring - The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Walter S. Harris, MBA, PMP
Deputy Commissioner for Operations
Chief Operating Officer

Date: 9/26/13