DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Assistant Secretary for Public Affairs
Washington, D.C. 20201

Case No.: 2015-01051-FOIA-OS

December 17, 2015

Aaron Boyd
Senior Writer
Federal Times
6883 Commercial Drive
Springfield, VA 22151

Dear Mr. Boyd:

This is the final response to your September 30, 2015, Freedom of Information Act (FOIA) request. Specifically, you requested the following: "records of network intrusion attempts on all HHS and component databases and servers, including security logs and documentation on major investigations from January 1, 2010 to September 30, 2015."

On or about December 2, 2015, you spoke by phone to Garfield Daley of my staff, and clarified your request. During the phone call, you indicated that you would prefer to receive the following information: "how many successful incidents occurred within HHS, where there were unauthorized access points for all HHS components (i.e. CDC, FDA, NIH, etc.) for at least a 30-day timeframe (increments) between January 1, 2010 and September 30, 2015. The access points include rout access, data exfiltration, and unauthorized access."

The Office of the Assistant Secretary for Administration, Office of the Chief Information Officer (ASA/OCIO) conducted a search for responsive records and located **111 pages**, available in Excel spreadsheet format. After a careful review of these pages, I have determined to release them to you in their entirety.

ASA/OCIO reports that from January 1, 2013 until June 30, 2015, the Department of Health and Human Services categorized incidents using Categories, as defined in the NIST Special Publication 800-61, rev.1. A list of the categories can be found on the References tab of the enclosed spreadsheet.

Beginning July 1, 2015, HHS converted from the legacy Category system to the Impact Classification system (defined in NIST SP800-61, rev.2 and expanded at https://www.us-cert.gov/incident-notification-guidelines). Impact Classifications consist of a four-factor matrix that provides a more descriptive picture of the impact of an incident on the Department.

Incidents that were created during the transition phase from Categories to Impact Classifications were dual-coded. These incidents are reported in the attached spreadsheet using only the official reporting mechanism, to prevent duplicate or extraneous reporting.

The Quantity provided represents the number of documented incidents that match the defining tuple preceding the value on that row. It should be assumed that if a possible tuple is not present, the value for that month is zero. The earliest month available with complete data is January 2013, due to document retention policies.

Document retention for incident data is based on General Records Schedule 24, item 7 (http://www.archives.gov/records-mgmt/grs/grs24.html). This item states that computer security incident handling records are to be "(d)estroyed/deleted 3 years after all necessary follow-up actions have been completed." See the Implementation Aid at the bottom of the website page for additional clarification.

There are no charges in this instance because the billable costs are less than our threshold of $25.

If you are not satisfied with this response, you may appeal. Your appeal must be mailed within 30 days from the date of receipt of this letter, to the official at the following address:

Ms. Catherine Teti
Deputy Agency Chief FOIA Officer
U.S. Department of Health and Human Services
Office of the Assistant Secretary for Public Affairs
200 Independence Avenue S.W.
Room 729H
Washington, DC 20201

Please clearly mark both the envelope and your letter “Freedom of Information Act Appeal.”

Sincerely yours,

Michael S. Marquis
Director
FOI/Privacy Acts Division

Enclosure(s)