Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

DEPARTMENT OF HEALTH AND HUMAN SERVICES HAD EMAIL REQUIREMENTS FOR POLITICAL APPOINTEES, BUT OFFICE OF THE SECRETARY LACKED EFFECTIVE MONITORING AND ENFORCEMENT

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Joanne M. Chiedi
Acting Inspector General

September 2019
A-18-18-11050

Office of Inspector General

https://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 nation-wide 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 healthcare industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: September 2019
Report No. A-18-18-11050

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Department of Health and Human Services Had Email Requirements for Political Appointees, but Office of the Secretary Lacked Effective Monitoring and Enforcement

Why OIG Did This Review

We conducted this audit in response to a congressional letter requesting a review of email usage by political appointees at HHS to ensure that "…officials are following the spirit and letter of all federal laws and regulations, as well as departmental policies, related to email use."

Our objectives were to determine whether HHS and its Operating Divisions (OpDivs) have controls in place to (1) restrict and monitor, in accordance with Federal laws and regulations, the use of personal email accounts to conduct Government business; and (2) preserve all emails related to Government activities as related to political appointees.

How OIG Did This Review

We reviewed applicable Federal laws, regulations, and guidance; reviewed training records of political appointees from the Office of the Secretary (OS) and four HHS OpDivs; gained an understanding of the current email security at HHS, OS, and selected OpDivs; and assessed the status of HHS's email program against policies, standards, and guidance.

We performed our audit field work from October 2017 through June 2018.

What OIG Found

We found that HHS had some controls in place to restrict and monitor the use of personal email accounts to conduct government business, in accordance with Federal laws and regulations, as well as policies and procedure to preserve all government emails on official email systems. However, three of the five HHS agencies/offices we audited did not have automated controls in place to block employees from accessing personal email accounts while logged into HHS, OS, or OpDiv networks. In addition, we found that OS did not ensure that all political appointees received security awareness training due to improper listing and classification of the political appointees.

What OIG Recommends and HHS Comments

We recommend that:

- HHS implement a policy requiring all HHS agencies and offices to implement automated controls to block employees from accessing personal email accounts from HHS networks;
- OS implement a process to ensure that all OS political appointees, employees, and contractors complete the required security awareness trainings in a timely manner; and
- OS implement procedures to ensure that its staff are properly listed and classified as political appointees, employees, contractors, and supervisors.

In written comments on our draft report, HHS concurred with our recommendations and described actions it plans to take to address our findings.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

We conducted this audit in response to a congressional request to review the email usage by political appointees at the Department of Health and Human Services (HHS) to verify that "officials are following the spirit and letter of all federal laws and regulations, as well as departmental policies, related to email use."

OBJECTIVES

Our objectives were to determine whether HHS and its Operating Divisions (OpDivs) have controls in place to (1) restrict and monitor, in accordance with Federal laws and regulations, the use of personal email accounts to conduct Government business; and (2) preserve all emails related to Government activities as related to political appointees.

BACKGROUND

The mission of HHS is to enhance the health and well-being of all Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.

HHS has 11 OpDivs, which administer HHS's programs. In addition, HHS has 18 staff divisions, which provide leadership, direction, and policy guidance to HHS.

HHS EMAIL USAGE

Email is commonly used for exchanging business information. To ensure that communications are adequately protected and preserved, HHS invests significant resources in cybersecurity,[1] data storage, servers, user training, and physical security. HHS requires employees to use Government email systems when using email to conduct Government business. Requirements for employee use of Government email systems are set forth in the *HHS Information Systems Security and Privacy Policy*, *HHS Policy for Records Management for Emails*, and *HHS Rules of Behavior for Use of HHS Information and IT Resources* (HHS RoB). Use of personal email for Government business presents risks to data privacy, record retention, and cybersecurity.

[1] The President's FY 2019 Budget appropriated $68 million to cybersecurity to protect sensitive and critical information in an ever-changing threat landscape.

HOW WE CONDUCTED THIS REVIEW

To accomplish our objectives, we reviewed applicable Federal laws, regulations, and guidance; reviewed training records of political appointees from the Office of the Secretary (OS)[2] and four HHS OpDivs;[3] gained an understanding of the current email security at HHS, OS, and selected OpDivs; and assessed the status of HHS's email program to determine whether the security program met policies, standards, and guidance.

We used a nonstatistical sample to evaluate the training records of 40 of 121 current political appointees at the time of our review from OS and 4 OpDivs. We reviewed the training records to determine whether the political appointees received required security training.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A describes our audit scope and methodology, and Appendix B contains Federal requirements and guidance for implementing controls needed to create, protect, and preserve email.

FINDINGS

We found that HHS had some controls in place to restrict and monitor the use of personal email accounts to conduct Government business, in accordance with Federal laws and regulations. However, three of the five HHS agencies/offices we audited (OS, ACF, and NIH) did not have automated controls in place to block employees from accessing personal email accounts while logged into HHS, OS, or OpDiv networks. This access occurred because HHS did not have a policy prohibiting it, and OS, ACF, and NIH had not assessed the risk of using personal email accounts. In addition, we found that OS did not ensure that all political appointees received security awareness training. (Among other things, this training covers the prohibition on using personal email to conduct Government business.) This occurred because OS lacked effective procedures to ensure that all staff take the required security awareness training. Without automated controls in place and completion of the required training, there was a heightened risk that employees could knowingly or unknowingly violate HHS policies by sending emails containing sensitive information or official business from personal email accounts using HHS networks. HHS did not have any reported incidents of personal email being used for such purposes from October 1, 2017, through June 30, 2018.

[2] OS is HHS's chief policy officer and general manager; it administers and oversees the organization, its programs, and its activities.

[3] Our audit covered the Administration for Children and Families (ACF), Centers for Disease Control and Prevention (CDC), Centers for Medicare & Medicaid Services (CMS), and National Institutes of Health (NIH).

We also found that HHS had policies and procedures in place to preserve all emails related to Government activities using official email systems. These policies and procedures have enabled HHS to effectively preserve emails and respond to, among other things, Freedom of Information Act (FOIA) requests.

HHS DID NOT HAVE A POLICY TO REQUIRE AUTOMATED CONTROLS TO BLOCK ACCESS TO PERSONAL EMAIL ACCOUNTS

We found that two of the five HHS agencies/offices (CMS and CDC) we audited blocked access to personal email websites from their networks (e.g., Gmail, Yahoo), which prevent employees from accessing personal email accounts. However, we found that OS, ACF, and NIH did not block access to personal email websites from their networks. This occurred, in part, because HHS did not have a policy requiring automated controls to block employees from accessing personal email accounts while logged into HHS, OS, or OpDiv networks. The decision as to whether to block access was left up to each of the HHS agencies/offices and without a requirement for the HHS agencies/offices to assess the associated risk to the agency/office and HHS.

Without a control in place to prevent employees from accessing personal email accounts, OS, ACF, and NIH increased the risk that employees, including political appointees, will use Government networks to access and use personal email accounts to conduct Government business. Personal email accounts generally do not have the same security or retention requirements as official Government email sites and could put personally identifiable information (PII) or other sensitive information at risk, either accidentally or intentionally. The HHS agencies/offices were also at risk of not being able to track or preserve the emails for purposes of detecting and responding to data breaches, responding to FOIA requests, records retention, and ensuring cybersecurity; this risk can be reduced by blocking employees' access to personal email accounts.

THE OFFICE OF THE SECRETARY DID NOT ENSURE THAT POLITICAL APPOINTEES RECEIVED REQUIRED SECURITY TRAINING

HHS officials stated that security awareness training and existing policies are the key controls in place to ensure that all employees, including political appointees, are not using personal email accounts to conduct official work. Also, all new HHS employees must attend an in-person cybersecurity briefing in which the trainer stresses that the use of personal email accounts to conduct HHS business is prohibited; web-based refresher security awareness training is provided on an annual basis thereafter. Supervisors must take additional security training. Further, in accordance with HHS policy, all employees, including political appointees, must sign the HHS RoB, which prohibits using personal email accounts to conduct official HHS business.

Of the 31 sampled OS political appointees, 23 did not complete the annual security awareness training and 13 were not listed on the tracking records as political appointees. In addition, 10 sampled OS political appointees who were supervisors did not receive required additional

security training for supervisors. Political appointees did not receive web-based annual security awareness training because of an oversight. Unlike the OpDivs (which used the HHS Learning Management System to track training), OS tracked training manually. Additionally, the political appointees who were supervisors did not receive the additional training they should have because they were not properly classified by OS as supervisors.

Users who have not received adequate security training may not follow security policies and therefore increase the risk of creating computer security incidents. This lack of training could lead to the loss, destruction, or misuse of sensitive Federal data assets. Without the required training, there is a heightened risk that employees knowingly or unknowingly violate HHS policies by using personal email accounts from HHS networks to conduct Government business.

HHS HAD NO REPORTED INSTANCES OF PERSONAL EMAIL BEING USED FOR OFFICIAL BUSINESS

HHS officials stated that neither the HHS Secretary nor any other HHS political appointees used personal email accounts to conduct Government business. For OS and the four OpDivs we audited, we requested any reported instances of personal email accounts being used for official business during October 1, 2017, through June 30, 2018. OS and the four OpDivs reported no instances of personal email accounts being used to conduct Government business.

HHS HAD POLICIES AND PROCEDURES IN PLACE TO PRESERVE ALL GOVERNMENT EMAILS ON OFFICAL EMAIL SYSTEMS

HHS guidance requires that emails related to Government activities or public policy be properly preserved as public records. *HHS Policy for Electronic Mail (Email) Records Management*, dated December 29, 2016, states that HHS will manage all email records in an appropriate electronic recordkeeping system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are required.

The HHS policy applies to all HHS OpDivs, staff divisions, and contractors conducting business for and on behalf of HHS through contractual relationships and service-level agreements. Email records (i.e., email messages and attachments, calendar appointments, and tasks captured by the electronic recordkeeping system) of designated capstone[4] officials must be retained permanently. This policy specifies an enhanced record retention standard that covers emails for all Senior Executive Service (SES), SES equivalents, and political appointees. Specifically, all SES, SES-equivalent, and political appointee emails will be auto-archived and retained indefinitely. For the five sampled HHS agencies/offices, we reviewed policies and procedures that each follows to preserve Government emails. We did not observe any weaknesses relating

[4] Capstone is an approach where OpDivs manage email records based on the role of the account holder rather than on the content of each email record.

to the policies and procedures in place for preserving and archiving emails relating to any employees, including political appointees.

HHS HAD POLICIES IN PLACE TO PRESERVE ALL EMAILS RELATED TO GOVERNMENT ACTIVITIES

HHS guidance requires that each OpDiv or staff division within HHS establish and maintain Federal record information contained in email or records transmitted by an electronic mail system. All sampled HHS agencies/offices stated that FOIA requests are processed through the HHS or the HHS agency's/office's FOIA office and are entered into a FOIA request tracking system for identification, tracking, and resolution. For example, when ACF receives a FOIA request, the request is sent to the Office of the Chief Information Officer, the entity that manages ACF email accounts. An official uses the Microsoft eDiscovery tool to search the mailboxes as requested by the search. The team performs a search according to the terms of the request and loads the results on the FOIA shared drive. The FOIA staff then loads the search results into the tracking system. The search results are reviewed by the FOIA staff within the tracking system and provided to the requester. We did not observe any weaknesses relating to emails being reviewed in response to FOIA requests.

RECOMMENDATIONS

We recommend that:

- HHS implement a policy requiring all HHS agencies and offices to implement automated controls to block employees from accessing personal email accounts from HHS networks;

- OS implement a process to ensure that all OS political appointees, employees, and contractors complete the required security awareness trainings in a timely manner; and

- OS implement procedures to ensure that all its staff are properly listed and classified in the categories of political appointees, employees, contractors, and supervisors.

HHS COMMENTS

In written comments to our draft report, HHS concurred with our recommendations and described actions it plans to take to address our findings.

HHS's comments are included as Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We limited our review to the policies and procedures at HHS, OS, and four OpDivs (ACF, CDC, CMS, and NIH) for restricting and monitoring, in accordance with Federal laws and regulations, the use of personal email accounts to conduct Government business and for preserving all emails related to Government activities. We selected a nonstatistical sample of 40 of 121 political appointees from OS and the 4 OpDivs and reviewed the training records of political appointees to verify required training was taken.

We performed our fieldwork in Washington, DC, from October 2017 through June 2018.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal laws, regulations, and guidance;
- evaluated the training records of 40 randomly selected political appointees from OS and the 4 OpDivs;
- interviewed relevant HHS, OS, and OpDiv personnel;
- gained an understanding of the current security program at HHS, OS, and selected OpDivs; and
- communicated our findings to HHS management.

We conducted these procedures in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS AND GUIDANCE

44 U.S.C. Chapter 31, Records Management by Federal Agencies

Section 3101 states that:

> The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

Section 3102 states that:

> The head of each Federal agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. The program, among other things, shall provide for:
>
> (1) effective controls over the creation and over the maintenance and use of records in the conduct of current business;
>
> (2) procedures for identifying records of general interest or use to the public that are appropriate for public disclosure, and for posting such records in a publicly accessible electronic format;
>
> (3) cooperation with the Archivist in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value; and
>
> (4) compliance with sections 2101–2117, 2501–2507, 2901–2909, and 3101–3107, of this title and the regulations issued under them.

36 CFR §1220.30(c)

This states that:

> Agency records management programs must provide for:
>
> (1) Effective controls over the creation, maintenance, and use of records in the conduct of current business; and

(2) Cooperation with the Archivist and the Administrator of [the General Services Administration] in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and destruction of records of temporary value.

45 CFR, Part 5 Freedom of Information Regulations (FOIA), Section 5.3

This states under the definition of "Office of the Secretary" that:

> HHS FOIA office within [The Office of the Assistant Secretary for Public Affairs] processes FOIA requests for records maintained by OS Staff Divisions other than the OIG. In certain circumstances and at the HHS FOIA Office's discretion, the HHS FOIA office may also process FOIA requests involving other HHS OpDivs.

HHS Information Systems Security and Privacy Policy, AC-20

This states that:

> Absent an agreement that establishes such terms, conditions, and trust relationships, employees and contractors are not to utilize unauthorized external information systems (such as personal email or personal online storage accounts) to conduct any Department business.

HHS Information Systems Security and Privacy Policy, adopted NIST SP 800-53 Revision 4, AT-2, Security Awareness Training Security Control

This states that:

> The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) (a) As part of initial training for new users (b) When required by system changes (c) and annually thereafter.

HHS Information Systems Security and Privacy Policy, adopted NIST SP 800-53 Revision 4, AT-3, Role-Based Security Training Security Control

This states that:

> The organization provides role-based security related training to all personnel with assigned significant responsibilities for information security: (a) before authorizing access to the system or performing assigned duties; (b) when required by system changes; and (c) within three (3) months of entering a

position that requires role-specific training, and at least once every three (3) years thereafter.

HHS Information Systems Security and Privacy Policy,

Appendix B

This states that OpDivs should:

a. Document and monitor individual information system security training activities, including basic security awareness training, specific information system security training and role-based security training; and

b. Retain individual training records for a minimum of five (5) years after completing a specific training course.

HHS Policy for Electronic Mail (Email) Records Management,

Section 3

This states that:

HHS will manage all email records in an appropriate electronic recordkeeping system that supports records management and litigation requirement (which may include preservation-in-place models), including the capability to identify, retrieve, and retain the records for as long as they are required.

Section 4

This states that:

The Capstone policy applies to all of HHS OpDivs, StaffDivs and contractors conducting business for, and on behalf of the Department through contractual relationships and service level agreements.

Section 5.1.3 (a)

This states that:

Email records (email messages and attachments, calendar appointments, and tasks captured by the electronic recordkeeping system) of designated capstone official's email accounts must be retained permanently.

NIST 800-45 Version 2

This states that:

> Personal email accounts are problematic, especially those accessed via a web browser that tend to bypass the email content filtering controls. In particular, if a user is using an SSL-encrypted[5] web page for personal email access and the organization does not decrypt and analyze SSL-encrypted HTTPS traffic, the content may be allowed out of or in even though it would not be if it went through normal channels.

[5] The Secure Socket Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser or a mail server and a mail client (e.g., Outlook).

APPENDIX C: HHS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Office of the Chief Information Officer
Washington, D.C. 20201

DATE: August 29, 2019

TO: Gloria L. Jarmon
Deputy Inspector General for Audit Services

FROM: José Arrieta JLA
Chief Information Officer

SUBJECT: OIG Draft Report: *The Department of Health and Human Services Had Email Requirements or Political Appointees; However, the Office of the Secretary Lacked Effective Monitoring and Enforcement,* A-18-18-11050

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for their review of the email requirements for political appointees. We welcome the opportunity to respond to the report.

As requested, our office has reviewed the aforementioned report and has attached written comments regarding the validity of facts, actions taken and planned actions, based on your recommendations. We look forward to continuing our collaboration efforts to enhance our policies and further implement safeguards and practices that protect HHS data and the health information of the American public.

If you have any questions or need additional information, please reach out to the Acting Chief Information Security Officer, Janet Vogel at Janet.Vogel@hhs.gov or 202-774-2446.

Attachment
TAB A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***The Department of Health and Human Services Had Email Requirements or Political Appointees; However, the Office of the Secretary Lacked Effective Monitoring and Enforcement,* A-18-18-11050**

CC:
Janet Vogel, Acting Chief Information Security Officer
Christopher Bollerer, Deputy Chief Information Security Officer
Jeffrey Arman, OIG Information Technology Audit Manager

TAB A: Response from the Office of the Chief Information Officer (OCIO) regarding ***The Department of Health and Human Services Had Email Requirements or Political Appointees; However, the Office of the Secretary Lacked Effective Monitoring and Enforcement,*** **A-18-18-11050**

Thank you for providing your draft recommendations resulting from OIG engagement, *A-18-18-11050, The Department of Health and Human Services Had Email Requirements for Political Appointees; However the Office of the Secretary Lacked Effective Monitoring and Enforcement.* Below please find our response to these draft recommendations.

OIG Recommendation 1:

We recommend that HHS implement a policy requiring all HHS agencies and offices to implement automated controls to block employees from accessing personal email accounts from HHS networks.

HHS Response: Concur

Various HHS operating divisions have implemented automated mechanisms to block access to and use of personal email accounts. OS has been and continues to assess these mechanisms for use within its environment. OS will continue to explore such mechanisms with the goal of implementing in FY20.

OIG Recommendation 2:

We recommend that OS implement a process to ensure that all OS political appointees, employees and contractors complete the required security awareness trainings in a timely manner.

HHS Response: Concur

OS will develop and implement a process to ensure that political appointees, employees and contractors have received initial security awareness trainings in a timely manner, and every year thereafter, per HHS policy.

OIG Recommendation 3:

We recommend that OS implement procedures to ensure that all its staff are properly listed and classified in the categories of political appointees, employees, contractors and supervisors.

HHS Response: Concur

OS will define clear categories of political appointees, employees, contractors and supervisors to ensure that all relevant staff are appropriately identified and categorized.