Department of Health and Human Services

**OFFICE OF INSPECTOR GENERAL**

# THE CENTERS FOR MEDICARE & MEDICAID SERVICES DID NOT ACCOUNT FOR NATIONAL SECURITY RISKS IN ITS ENTERPRISE RISK MANAGEMENT PROCESSES

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

July 2021
A-18-20-06200

# *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 nationwide network of audits, investigations, and inspections conducted by the following operating components:

## *Office of Audit Services*

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

## *Office of Evaluation and Inspections*

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

## *Office of Investigations*

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

## *Office of Counsel to the Inspector General*

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

# *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 website.

**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: July 2021
Report No. A-18-20-06200

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

# The Centers for Medicare & Medicaid Services Did Not Account for National Security Risks in Its Enterprise Risk Management Processes

**Why OIG Did This Audit**
We conducted this audit in response to a congressional request to determine whether the Centers for Medicare & Medicaid Services' (CMS's) enterprise risk management (ERM) process includes steps to identify and assess national security risks. The congressional request was prompted by a previous OIG audit that determined that national security risks were not adequately considered by the National Institutes of Health (NIH). Specifically, we found that NIH did not consider the risk presented by foreign principal investigators when permitting access to United States genomic data. The Congressmen stated that they are concerned that CMS also has not considered national security risks to its programs.

Our objective was to determine whether CMS's ERM process considered national security risks to all CMS programs in accordance with Federal requirements.

**How OIG Did This Audit**
We reviewed CMS's ERM process and risk assessment policies and procedures, reviewed additional supporting risk management documentation, and interviewed CMS and HHS personnel.

**What OIG Found**
CMS's ERM process did not consider national security risks for any of CMS's programs in accordance with Federal requirements. CMS lacked policies and procedures that required its programs to consider national security threats because it relied on HHS's ERM process. As a result, CMS was unable to ensure that it had implemented effective controls to protect against threats from foreign and domestic adversaries.

**What OIG Recommends and CMS's Comments**
We recommend that CMS, as part of its ERM program, implement a process to assess all of its programs for national security risks in accordance with OMB Circular No. A-123's requirement to include new or emerging risks in the risk profile.

In written comments to our draft report, CMS concurred with our recommendation. CMS also stated that it currently participates in the HHS enterprise risk management process, is in the early stages of establishing an agency enterprise risk management program, and will consider how to assess national security risks across its programs.

**TABLE OF CONTENTS**

# INTRODUCTION

## WHY WE DID THIS AUDIT

We conducted this audit in response to a congressional request to determine whether the Centers for Medicare & Medicaid Services' (CMS's) enterprise risk management (ERM) process includes steps to identify and assess national security risks.[1] The congressional request was prompted by a previous Office of Inspector General audit that determined that national security risks were not adequately considered by the National Institutes of Health (NIH).[2] Specifically, we found that NIH did not consider the risk presented by foreign principal investigators when permitting access to United States genomic data. The Congressmen stated that they are concerned that CMS also has not considered national security risks to its programs.

## OBJECTIVE

Our objective was to determine whether CMS's ERM process considered national security risks to all CMS programs in accordance with Federal requirements.

## BACKGROUND

### Centers for Medicare & Medicaid Services

CMS, which is part of the Department of Health and Human Services (HHS), oversees Medicare, Medicaid, and other programs. These programs are responsible for protecting large volumes of sensitive health data.[3]

### HHS Office of National Security

Created in 2002, the HHS Office of National Security (ONS) is responsible for integrating intelligence and security information into HHS policy and operational decisions. As the HHS Federal Senior Intelligence Coordinator, ONS works with other Federal departments and

---

[1] "Enterprise Risk Management is an effective agencywide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio rather than addressing risks only within silos." Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Issued July 15, 2016.

[2] *Opportunities Exist for the National Institutes of Health To Strengthen Controls in Place To Permit and Monitor Access to Its Sensitive Data.* Issued February 5, 2019. Access online at https://oig.hhs.gov/oas/reports/region18/181809350.pdf.

[3] CMS's information systems process millions of highly sensitive pieces of information, including personally identifiable information (PII), protected health information (PHI), and Federal Tax Information (FTI) records. (The CMS Cyber Threat Intelligence *Operations Standard Operating Procedures,* dated Jan. 16, 2019.)

agencies, including law enforcement organizations, to protect HHS and its information from national security threats. ONS also works with HHS's operating divisions as part of the HHS Insider Threat Program. ONS officials stated that ONS considers the protection of program beneficiaries' personally identifiable information (PII), which includes genomic data, to be a national security concern. ONS also considers divulging PII to a foreign adversarial State to be a national security breach.

## HOW WE CONDUCTED THIS AUDIT

We reviewed CMS's ERM process and risk assessment policies and procedures, reviewed additional supporting risk management documentation, and interviewed CMS and HHS personnel.

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.

The Appendix contains the details of our scope and methodology.

## FINDINGS

CMS's ERM process did not consider national security risks for any CMS programs in accordance with Federal requirements. CMS lacked policies and procedures that required its programs to consider national security threats because it relied on HHS's ERM process. As a result, CMS was unable to ensure that it had implemented effective controls to protect against threats from foreign and domestic adversaries.

## CMS DID NOT ASSESS NATIONAL SECURITY RISKS FOR ANY OF ITS PROGRAMS

The Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* requires that agencies, at least annually, prepare or update their complete risk profile and include required risk components and elements.[4] The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an agency faces in attempting to attain its strategic objectives and to identify appropriate options for addressing the significant risks faced by programs. When conducting risk assessment, an agency should identify internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, the agency should take into account relevant interactions within the organization as well as with outside organizations. As

[4] A risk profile is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process.

part of the risk profile's identification of risk step, agencies are required to conduct continuous risk identification in order to identify new or emerging risks.

CMS did not generate an agency risk profile as a component of its ERM program. Instead, CMS relied on HHS's Department-level ERM process, which did not include detailed analysis of the risks CMS and its programs faced. Although some CMS programs have access to PII and other sensitive data that adversaries may attempt to access, CMS policies and procedures did not mandate that programs consider national security risks, even though ONS had advised all HHS agencies, to include CMS, that national security is a new or emerging risk. CMS's Clinical Laboratory Improvement Amendments (CLIA) program, which oversees and regulates approximately 260,000 non-research testing laboratories in the United States and internationally[5], is an example of a program that could benefit from an assessment of national security risks. By not assessing national security risks and implementing mitigating controls, CMS programs and their related data are vulnerable to foreign and domestic adversarial threats.

## RECOMMENDATION

We recommend that the Centers for Medicare & Medicaid Services, as part of its ERM program, implement a process to assess all of its programs for national security risks in accordance with OMB Circular No. A-123's requirement to include new or emerging risks in the risk profile.

## CMS COMMENTS

In written comments to our draft report, CMS concurred with our recommendation. CMS also stated that it currently participates in the HHS enterprise risk management process, is in the early stages of establishing an agency enterprise risk management program, and will consider how to assess national security risks across its programs. CMS's response is included in its entirety as Appendix B.

## OIG RESPONSE

We are encouraged that CMS has taken steps to further safeguard its programs and their related data against new or emerging risks, including national security risks.

[5] Non-research testing laboratories examine "materials derived from the human body for the purpose of providing information for the diagnosis, prevention, or treatment of any disease or impairment of, of the assessment of the health of, human beings" (42 CFR § 493.2).

## APPENDIX A: AUDIT SCOPE AND METHODOLOGY

**SCOPE:**

We reviewed the CMS ERM process, risk assessment policies, HHS's policies and procedures related to assessing and addressing foreign and domestic threats, and additional supporting documents provided by CMS, and interviewed CMS and HHS personnel. We conducted our audit work from January 2020 through May 2021.

**METHODOLOGY:**

To accomplish our objective, we:

- reviewed applicable Federal regulations and guidance;
- reviewed CMS's ERM policies, procedures, and practices;
- reviewed CMS's documentation related to its information security risk assessments, insider threat implementation plan, and national security information policy;
- interviewed CMS officials;
- interviewed HHS officials, including those at ONS; and
- discussed our findings with CMS officials.

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 B: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

*Administrator*
Washington, DC 20201

**DATE:** June 17, 2021

**TO:** Amy J. Frontz
Deputy Inspector General for Audit Services
Office of Inspector General

**FROM:** Chiquita Brooks-LaSure
Administrator
Centers for Medicare & Medicaid Services

**SUBJECT:** Office of Inspector General (OIG) Draft Report: The Centers for Medicare & Medicaid Services Did Not Account for National Security Risks in Its Enterprise Risk Management Processes (A-18-20-06200)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report.

The security of CMS systems and patient data is a top priority for CMS. CMS's Office of Strategy, Performance, and Results oversees and is accountable for the development of an enterprise risk management (ERM) function that will provide risk analysis, assessment, and mitigation services to support CMS functions. Ensuring tight coupling with agency strategic priorities, this capability will amplify the many component level risk management activities already underway to an enterprise perspective. As noted in the OIG's report, CMS currently participates in the Department of Health & Human Services (HHS) enterprise risk management process to support efforts across the department and is currently assessing how best to integrate CMS's cybersecurity and national security risks into an agency enterprise risk management program.

To secure against potential vulnerabilities, CMS vigilantly monitors, tests, and strengthens its systems against cyber-attacks, both foreign and domestic, and has procedures and processes in place to quickly identify, mitigate, and remove threats, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) requirements and guidelines issued by the United States Computer Emergency Readiness Team (US-CERT). Since 2015, CMS has participated in the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program, which is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first.

CMS's Office of Information Technology provides guidance and oversight for protecting the confidentiality, integrity, and availability of CMS's information and information systems. CMS collects and analyzes threat intelligence, develops threat responses, tracks threat remediation

activities, and receives third party threat intelligence and reports on program operations. The Office of Information Technology also supports business and system owners across CMS by developing and implementing counterintelligence, insider threat, supply chain risk management and Committee on Foreign Investment in the United States (CFIUS) programs. These programs serve to identify and prevent the exploitation of CMS personnel, information, and assets by foreign intelligence and security services, terrorists, or transnational criminal organizations working under the direction of a foreign entity. Once mature these programs will identify and monitor threats, assess vulnerabilities in CMS contracts, and mitigate the potential impact from loss of sensitive or restricted information or damage to critical infrastructure by both insiders and foreign adversaries.

OIG's recommendations and CMS's responses are below.

**OIG Recommendation**

The OIG recommends that CMS, as part of its ERM program, implement a process to assess all of its programs for national security risks in accordance with OMB Circular No. A-123's requirement to include new or emerging risks in the risk profile

**CMS Response**

CMS concurs with this recommendation. CMS currently participates in the HHS enterprise risk management process to support efforts across the department. In addition, CMS is in the early stages of establishing an agency enterprise risk management program and will consider how to assess national security risks across its programs as part of this effort.