



DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201



FOIA Request 2022-0233

Freedom of Information Act Office
Cohen Bldg., Suite 5527
330 Independence Ave., SW
Washington DC 20201

August 24, 2022

By Email.

Nate Jones
The Washington Post
1301 K Street NW
Washington DC 20071
Email: Nate.Jones@washpost.com

Dear Nate Jones:

This is in response to the undated Freedom of Information Act ("FOIA") request you originally submitted to the Department of Health and Human Services ("HHS"), and received in the Office of Inspector General ("OIG") on November 16, 2021, seeking a copy of OIG Audit Report *"Two Critical HHS Systems Were Deployed Without Authorizations to Operate."*


The Office of Audit Services located thirty-five (35) pages responsive to your request; I have determined to release all thirty-five (35) pages without deletion.

I trust this information fully satisfies your request. If you need any further assistance or would like to discuss any aspect of your request, please do not hesitate to contact our FOIA Requester Service Center at 202.619.2541 or email at FOIA@oig.hhs.gov.

There is no charge for FOIA services in this instance because billable fees are under the Department's \$25 cost effective threshold.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

Sincerely,


Robin R. Brooks
Director
Freedom of Information



DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201



August 24, 2022

TO: Karl S. Mathias, Ph.D.
Chief Information Officer
Department of Health and Human Services

FROM: Amy J. Frontz
Deputy Inspector General for Audit Services

SUBJECT: Rescission of Department of Health and Human Services, Office of Inspector General Final Report *HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls*, A-18-20-06800, November 2, 2021

In accordance with Generally Accepted Government Auditing Standards, we are notifying you that the subject report has been rescinded and you should discontinue relying on the information contained therein. Based on information and documentation obtained by OIG after the completion of this audit, we concluded that some of the information and application of criteria in the audit regarding the U.S. Healthcare COVID-19 Portal, referred to as TeleTracking in the report, is inaccurate. The report was not posted on our website; however, the modified report title and report number, which were posted on our website, will be removed and replaced with this memo. Any copies of the report in your possession should be destroyed.

Upon completion of additional audit work, we will re-issue a revised report under number A-18-20-06800R. The revised report will describe the results of our assessment of HHS's compliance with the applicable criteria for the U.S. Healthcare COVID-19 Portal at the time HHS initiated use of the portal. The revised report will also incorporate information provided to the audit team after the publication of the subject report and any other revisions determined to be necessary.



DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20201



November 2, 2021

TO: Janet Vogel
Acting Chief Information Officer
Department of Health and Human Services

FROM: Christi A. Grimm
Principal Deputy Performing Duties of the Inspector General

CHRISTI GRIMM Digitally signed by
CHRISTI GRIMM
Date: 2021.11.02
13:51:36 -04'00'

SUBJECT: OIG Final Report: *HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls*, A-18-20-06800

The attached final report provides the results of our audit of HHS Protect and TeleTracking foundational cybersecurity controls to ensure the integrity and availability of the systems.

This report contains restricted, sensitive information that may be exempt from release under the Freedom of Information Act, 5 U.S.C. § 552. The report will not be posted on the internet. If information in the report is released pursuant to a request under the Act, the restricted, sensitive information and other information exempt from release will be redacted.

If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Tamara Lilly, Assistant Inspector General for Audit Services, at (202) 802-0411 or Tamara.Lilly@oig.hhs.gov. We look forward to receiving your final management decision within 6 months. Please refer to report number A-18-20-06800 in all correspondence.

Attachment

cc:
Christopher Bollerer
Acting Chief Information Security Officer
Department of Health and Human Services

Warning— This report contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). If disclosed, the information in this report could adversely affect information security on U.S. Government Systems. Distribution should be strictly limited to authorized officials. Do not reproduce or release to any person without prior approval from the Department of Health and Human Services, Office of Inspector General, Office of Audit Services.

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**HHS PROTECT AND
TELETRACKING WERE
LAUNCHED WITHOUT
FOUNDATIONAL CYBERSECURITY
CONTROLS**

**WARNING: THIS REPORT CONTAINS RESTRICTED, SENSITIVE
INFORMATION, SUCH AS CONFIDENTIAL PROPRIETARY
MATERIAL WITH A HIGH POTENTIAL FOR MISUSE.
DISTRIBUTION SHOULD BE STRICTLY LIMITED. DO NOT
REPRODUCE OR RELEASE TO ANY PERSON WITHOUT THE
PRIOR APPROVAL OF THE OFFICE OF AUDIT SERVICES.**



Christi A. Grimm
Principal
Deputy Inspector General

**November 2021
A-18-20-06800**

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 CONTAINS RESTRICTED INFORMATION

This report should not be reproduced or released to any other party without specific written approval from OAS.

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: November 2021

Report No. A-18-20-06800

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



Why OIG Did This Audit

The Department of Health and Human Services (HHS) deployed HHS Protect and its component system, the U.S. Healthcare COVID-19 Portal (TeleTracking), to collect and report critical data from States, communities, and hospitals to be used in the Federal response to the COVID-19 pandemic. Throughout the pandemic, HHS and other entities serving an integral role in the COVID-19 response have been subjected to significant cybersecurity threats and attacks. Ensuring that systems supporting the COVID-19 response have implemented foundational cybersecurity controls is important to the integrity and availability of critical public health data.

Our objective was to determine whether HHS has implemented foundational cybersecurity controls to ensure the integrity and availability of HHS Protect and TeleTracking.

How OIG Did This Audit

We focused on determining whether HHS designed and implemented cybersecurity controls that are foundational to securing HHS Protect and its TeleTracking component prior to deployment. To accomplish our objective, we requested and reviewed HHS's cybersecurity controls documentation related to ensuring the integrity and availability of HHS Protect and TeleTracking.

HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls

What OIG Found

Select cybersecurity controls that are foundational to ensuring the integrity and availability of HHS Protect and TeleTracking were not implemented prior to the deployment of the systems. Cybersecurity controls for both systems were not implemented prior to deployment because HHS officials prioritized deploying the systems for operational use to achieve the agency's mission of combating the COVID-19 pandemic before meeting Federal requirements. When deployed, the systems were susceptible to an unknown and possibly unacceptably high risk of failure or compromise from unintentional disruptions or cyberattacks. For example, HHS had not conducted a risk assessment for HHS Protect. Without a risk assessment, management may not identify potential threats and develop proper measures to ensure HHS Protect and its components are protected.

Given the likelihood that HHS will be called upon to respond to future public health emergencies, developing a streamlined process to rapidly develop, assess, formally authorize, and deploy an IT system with the required foundational cybersecurity controls will better prepare HHS to respond to such emergencies and thwart potential IT disruptions and cyber threats.

What OIG Recommends and HHS Comments

We recommend that HHS:

- reperform the security categorization of HHS Protect to factor in personally identifiable information and update cybersecurity controls if necessary;
- complete implementation and testing of required cybersecurity controls for the HHS Protect system based on the appropriate security categorization, including the risk assessment and IT contingency plan;
- complete implementation and testing of required cybersecurity controls for the TeleTracking system based on the appropriate security categorization; and
- develop a streamlined process to identify, implement, and test cybersecurity controls for new IT systems that are rapidly deployed to meet a mission-critical need.

HHS did not concur with our first three recommendations and concurred with the fourth recommendation. HHS also provided technical comments, which we addressed as appropriate. We maintain that our findings and recommendations are accurate and valid.

TABLE OF CONTENTS

INTRODUCTION	1
Why We Did This Audit	1
Objective	1
Background	2
COVID-19 Timeline	2
Role of HHS in Emerging Infectious Disease Preparation and Response	2
Public Health Data Reporting.....	2
HHS Protect	3
TeleTracking	4
How We Conducted This Audit	4
FINDINGS.....	6
Required Controls Were Not Implemented Prior to the Deployment of HHS Protect and Some Controls Remain Unimplemented	7
PII Not Factored Into System Categorization.....	7
HHS Protect Did Not Have a Risk Assessment and an IT Contingency Plan	8
HHS Protect Lacked Authorization To Operate	8
TeleTracking Foundational Controls Were Not Implemented Prior to Deployment and Remain Unimplemented.....	9
HHS Did Not Have a Process for Ensuring Cybersecurity of Rapidly Developed Systems.....	10
RECOMMENDATIONS	11
HHS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE.....	12
Reperform the Security Categorization of HHS Protect	12
HHS Comments	12
OIG Response	12

HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls (A-18-20-06800)

Warning—This report contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. § 522). If disclosed, the information in this report could adversely affect information security on U.S. Government Systems. Distribution should be strictly limited. Do not reproduce or release to any person without prior approval from the Department of Health and Human Services, Office of Inspector General, Office of Audit Services.

Ensure Cybersecurity of HHS Protect and TeleTracking	13
HHS Comments	13
OIG Response	13

APPENDICES

A: Audit Scope and Methodology	14
B: Federal Requirements and Guidance	15
C: Security Document Review Tables	19
D: HHS Comments.....	23

HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls (A-18-20-06800)

Warning—This report contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. § 522). If disclosed, the information in this report could adversely affect information security on U.S. Government Systems. Distribution should be strictly limited. Do not reproduce or release to any person without prior approval from the Department of Health and Human Services, Office of Inspector General, Office of Audit Services.

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS) deployed HHS Protect and its component system, the U.S. Healthcare COVID-19 Portal (TeleTracking), to collect and report critical data from States, communities, and hospitals to be used in the Federal response to the COVID-19 pandemic. HHS Protect and TeleTracking data is used by Federal, State, Tribal, and local governments to track the movement of the virus, identify potential stresses on the health care delivery system, and manage the distribution of supplies. Throughout the pandemic, HHS and other entities serving an integral role in the COVID-19 response have been subjected to significant cybersecurity threats and attacks. Ensuring that systems such as HHS Protect and TeleTracking that support the COVID-19 response have implemented foundational cybersecurity controls is important to ensuring the integrity and availability of critical public health data.¹

OBJECTIVE

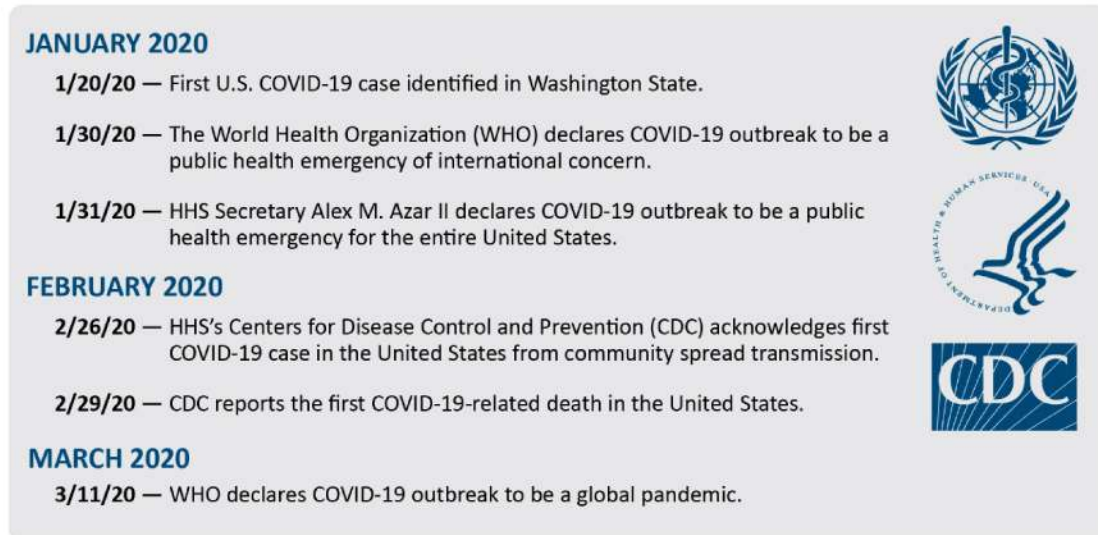
Our objective was to determine whether HHS implemented foundational cybersecurity controls in order to ensure the integrity and availability of HHS Protect and TeleTracking.

¹ Foundational cybersecurity controls are the starting point for achieving effective cybersecurity. These controls serve as the foundation for subsequent controls before a system reaches the production stage.

BACKGROUND

COVID-19 Timeline

Figure 1: Initial Progression of COVID-19 in the United States



Role of HHS in Emerging Infectious Disease Preparation and Response

HHS is the primary Federal department responsible for medical support and coordination during public health emergencies, including the COVID-19 pandemic.² The Office of the Chief Information Officer (OCIO) supports the HHS mission by leading the development and implementation of information technology infrastructure across the agency. Operating divisions (OpDivs) and staff divisions (StaffDivs) involved in the COVID-19 pandemic response include the Office of the Assistant Secretary for Preparedness and Response (ASPR), Centers for Disease Control and Prevention (CDC), Centers for Medicare & Medicaid Services, Food and Drug Administration, and Health Resources and Services Administration.

Public Health Data Reporting

The COVID-19 pandemic has demonstrated the importance of having access to timely, accurate, and comprehensive public health data. Prior to the pandemic, national public health data reporting had not been modernized, often relied on multiple layers of government reporting,

² Federal Emergency Management Agency, "Emergency Support Function #8—Public Health and Medical Services Annex," June 2016. Accessed at https://www.fema.gov/sites/default/files/2020-07/fema_ESF_8_Public-Health-Medical.pdf on June 3, 2021.

and was burdensome for health care providers and others involved in direct public health response efforts.³ In addition, CDC began its Data Modernization Initiative to improve public health data, technology, and workforce capabilities. Congress provided CDC funding for public health modernization efforts in COVID-19-related relief bills.⁴ And a recent Executive Order (EO) also directed Federal agencies to improve COVID-19-related data efforts, which include facilitating the gathering, sharing, and reporting of public health data.⁵

HHS Protect

At the start of the pandemic, HHS OpDivs and StaffDivs were separately collecting COVID-19-related data. HHS leadership and the White House COVID-19 task force both concluded that data collection efforts needed to be improved. In response, HHS deployed the HHS Protect system on April 10, 2020, to centralize data collection and reporting related to the pandemic.

According to HHS, HHS Protect receives and integrates data from more than 200 disparate data sources that include Federal, State, and local governments and the health care industry. HHS Protect was deployed with the goal of providing a comprehensive view of the U.S. health care system so that decisionmakers would have access to near real-time information. HHS Protect was intended to provide, among other things, authorized users access to hospital-specific data such as:

- hospital capacity, utilization, and inventory data;
- COVID-19 case counts;
- supply chain data;
- testing data; and
- population and demographic data.

³ [HHS Protect: Frequently Asked Questions | HHS.gov](#). Accessed June 20, 2020.

⁴ Cares Act, P.L. 116-136 (Mar. 27, 2020); American Rescue Plan Act of 2021, P.L. 117-2 (Mar. 11, 2021).

⁵ Executive Order on Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats (Jan. 21, 2021). Accessed at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-ensuring-a-data-driven-response-to-covid-19-and-future-high-consequence-public-health-threats/> on June 3, 2021.

TeleTracking

In March 2020, ASPR awarded a 6-month contract to TeleTracking Technologies, Inc., to provide HHS with a system for real-time hospital capacity reporting related to COVID-19 pandemic efforts. The TeleTracking system is a component of HHS Protect that enables HHS to streamline hospital data collection, quickly create new data fields, and collect nationwide data within 3 days, according to HHS officials. On July 15, 2020, at the direction of HHS, hospitals began to input their data in TeleTracking or via their respective State health departments instead of CDC's National Healthcare Safety Network (NHSN) to reduce confusion and reporting duplication. TeleTracking has provided HHS with access to data from an additional 1,100 hospitals.⁶ In March 2021, HHS awarded TeleTracking Technologies a third, 6-month contract to continue its work with HHS for the period of April 2021 through September 2021.

HOW WE CONDUCTED THIS AUDIT

We focused on determining whether HHS designed and implemented cybersecurity controls that are foundational to securing HHS Protect and its TeleTracking component prior to deployment. To accomplish our objective, we requested and reviewed HHS's cybersecurity controls documentation related to ensuring the integrity and availability of HHS Protect and TeleTracking. We also interviewed HHS personnel and observed certain system cybersecurity controls in use during a demonstration of the two systems' capabilities.

We assessed select HHS Protect and TeleTracking foundational cybersecurity controls to determine compliance with the requirements of the National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

The following are the cybersecurity controls we selected and reviewed for this audit:

- Authorization to Operate (ATO) – The official management decision given by a senior organizational official to authorize operation of an IT system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

⁶ According to HHS, NHSN received COVID-19 data from 3,000 of the approximately 6,200 hospitals across the United States.

- Contingency Plan and Testing – The plan to maintain or restore IT systems that support essential agency missions and business operations despite a disruption, disaster, compromise, or failure (natural or man-made) and testing to determine the effectiveness of the plan and the organizational readiness for executing the plan.
- Risk Assessment – The process of identifying and documenting the risks to an organization’s operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation of the information system. It is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
- Privacy Impact Assessment – An analysis and documenting of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- Security Categorization – The process of determining the characterization of an information system or its information based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation. Using this process, the information or information system is categorized as low impact, moderate impact, or high impact, and this categorization process determines the security controls that should be designed and implemented to ensure its confidentiality, integrity, and availability.
- System Security Plan – The formal document that provides an overview of the security requirements for an IT system and describes the security controls in place or planned for meeting those requirements.
- Vulnerability Assessment – A systematic examination of an IT system or product to determine the adequacy of security measures, identify deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Our audit was designed to determine whether these cybersecurity controls were implemented prior to the deployment of HHS Protect and its TeleTracking component for operational use in

accordance with Federal requirements; our audit was not an assessment of all organizational internal or IT controls.

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 objective.

Appendix A contains the details of our scope and methodology, and Appendix B contains Federal requirements and guidance.

FINDINGS

Select cybersecurity controls that are foundational to ensuring the integrity and availability of HHS Protect and TeleTracking were not implemented prior to the deployment of the systems. For HHS Protect, HHS had not completed a privacy impact assessment (PIA), risk assessment, security categorization process, security plan, vulnerability assessment, or contingency plan. Additionally, the authorization for the system to operate for official use had not been issued prior to the system's deployment. HHS implemented four of the six foundational cybersecurity controls after HHS Protect was deployed. HHS also granted HHS Protect an authorization to operate without conditions 9 months after its deployment on January 20, 2021. As of March 3, 2021, TeleTracking had not been granted authorization to operate for official use and two cybersecurity controls remained unimplemented.

When deployed, the systems were susceptible to an unknown and possibly unacceptably high risk of failure or compromise from unintentional disruptions (e.g., man-made or natural disasters) or cyberattacks. Although HHS had not reported a major incident for HHS Protect or TeleTracking during our audit period, HHS systems continued to be prime targets of cyberattacks. If an attack had been successful, the systems or data could have been potentially destroyed or compromised and HHS may have been unable to restore the systems or data in a timely manner, which would have significantly hindered critical pandemic response efforts.

Cybersecurity controls for both systems were not implemented prior to deployment because HHS officials prioritized deploying the systems for operational use to achieve the agency's mission of combating the COVID-19 pandemic over meeting all the Federal requirements prior to its deployment. Additionally, HHS did not have a streamlined version of the traditional assessment and authorization process that could be used to rapidly deploy an IT system.

REQUIRED CONTROLS WERE NOT IMPLEMENTED PRIOR TO THE DEPLOYMENT OF HHS PROTECT AND SOME CONTROLS REMAIN UNIMPLEMENTED

When HHS officials launched HHS Protect on April 10, 2020, it had not implemented some foundational security controls and based its assurance that other controls were properly implemented on incomplete testing. Specifically, the PIA, security categorization, risk assessment, and contingency plan had not been completed prior to the system's launch. Additionally, the written authorization for the system to operate had not been issued prior to the system's deployment. OCIO officials explained that some cyber assessments had been conducted on an ad hoc basis prior to launch, and they believed based on their expertise that HHS Protect was secure when it was deployed. However, we could not verify that OCIO performed cyber assessments because documentation was not generated. Although HHS later implemented four foundational cybersecurity controls, as of March 3, 2021, it still had not completed a risk assessment and contingency plan.

PII Not Factored Into System Categorization Process

Prior to HHS Protect deployment, the PIA and system categorization process had not been completed. These controls are required to be completed prior to a system's deployment for operational use, according to NIST SP 800-53, Revision 4. The PIA and system categorization process play an important role in identifying the appropriate controls to protect the system and its data from misuse and abuse. Without completing and knowing the PIA results and system categorization process, HHS implemented security controls that it believed were adequate.

Subsequent to our audit request for the PIA and categorization process documentation, HHS took action to complete both. A PIA is designed to identify and mitigate privacy risks. Specifically, a PIA informs the public of the personal identifiable information (PII) being collected, why it is being collected, and how it will be used, accessed, shared, safeguarded, and stored. The PIA completed on September 16, 2020, indicated that HHS Protect contains PII. Our review of the security categorization process documentation found that the use of PII by HHS Protect did not appear to be considered in the system categorization process as it should have been. Additionally, we found that the HHS Protect conditional authorization to operate memo dated August 18, 2020, incorrectly stated that HHS Protect did not collect, store, or transmit any PII despite the results of the PIA. If PII is contained in the system and not factored into the categorization process, there is an increased risk of improperly categorizing the system or data and selecting the inappropriate cybersecurity controls for implementation. Absent or inadequate security controls expose the processing, storage, or transmission of PII and may result in cyber attackers or disgruntled employees stealing, destroying, or inappropriately disclosing PII. This means that HHS's inconsistent determination as to whether HHS Protect

contains PII could lead to unintentional disclosure or destruction of PII or other sensitive information.

HHS Protect Did Not Have a Risk Assessment and an IT Contingency Plan

HHS had not conducted a risk assessment or completed a contingency plan for HHS Protect prior to its launch for operational use. NIST SP 800-30 *Guide for Conducting Risk Assessments* describes a “risk assessment” as the process by which “leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage” NIST SP 800-30 also states that a risk assessment includes the following steps: framing the risk, assessing the risk, responding to the risk, and monitoring the risk. Without a risk assessment, management may not identify potential threats and develop proper measures to ensure HHS Protect and its components are protected. NIST SP 800-34, Revision 1 *Contingency Planning Guide for Federal Information Systems* describes a contingency plan as having established procedures for the assessment and recovery of a system following a system disruption.

At the time of our audit, HHS had not completed any of these steps for HHS Protect. The contingency planning process is critical to ensuring that systems remain available after natural and man-made disasters. Importantly, without a contingency plan HHS may not be prepared to recover from certain types of cyberattacks (such as ransomware and denial of service), which could result in a loss of data or lack of access to information for decisionmakers.

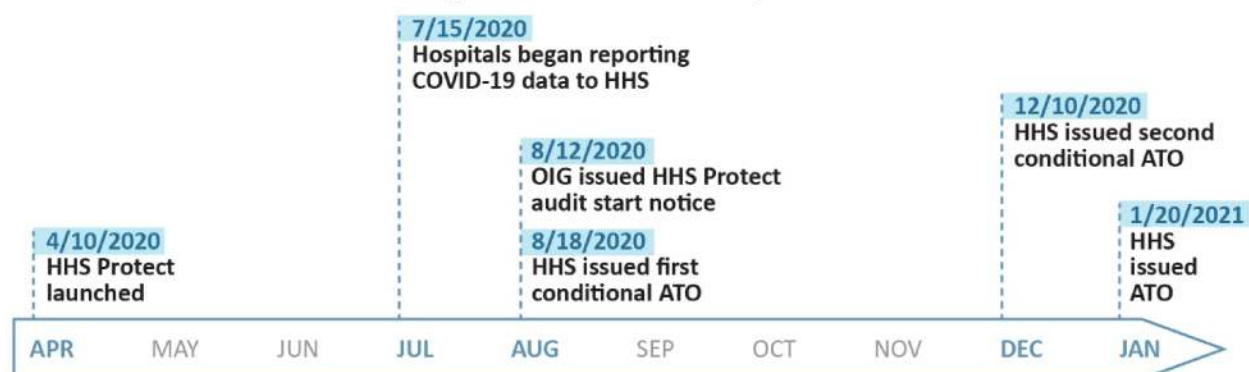
HHS Protect Lacked Authorization To Operate

HHS launched HHS Protect on April 10, 2020, prior to completing the authorization process and documenting the responsible HHS official’s authorization to operate for official use. The Office of Management and Budget (OMB) Circular No. A-130, *Appendix III: Security of Federal Automated Information Resources*, Section A(3)(b)(4) requires that Federal agencies ensure that a management official authorizes in writing the use of the application by confirming that its security plan as implemented adequately secures the application. HHS management made the decision not to complete an authorization to operate because it prioritized making HHS Protect operational to combat the public health crisis before completing cybersecurity requirements. Without the federally required authorization to operate, there is no assurance that HHS management has assessed cybersecurity risk associated with HHS Protect, which puts public health data at increased risk for unauthorized disclosure or manipulation, as well as a cyberattack.

On August 18, 2020—four months after HHS Protect was deployed—HHS officials signed a memo that granted a “conditional” authorization to operate the system for official use. The memo acknowledged that the required full cybersecurity assessment had not been completed

and “a substantial amount of documentation that would typically corroborate system security” did not exist. This conditional memo was not retroactive to the date the system was deployed. Instead, it authorized the system to operate for an additional 120 days (through December 16, 2020) to give HHS time to complete a full cybersecurity assessment. On December 10, 2020, a second 120-day extension was granted, again noting the lack of completed security documentation. On January 20, 2021, nine months after deploying the system, an authorization memo without conditions was signed that granted permission for HHS Protect to operate for official use. (See Figure 2 for a timeline of key dates.) However, as of March 3, 2021, HHS still had not completed two of the foundational cybersecurity controls—a risk assessment and a contingency plan—for HHS Protect.

Figure 2: HHS Protect Key Dates



Appendix C contains further details on our analysis of the HHS Protect cybersecurity documentation.

TELETRACKING FOUNDATIONAL CONTROLS WERE NOT IMPLEMENTED PRIOR TO LAUNCH AND REMAIN UNIMPLEMENTED

When HHS placed TeleTracking into production, it had not completed the PIA, risk assessment, security categorization, security plan, vulnerability assessment, or contingency plan cybersecurity controls. Additionally, the written authorization for the system to operate for official use had not been issued prior to the system’s deployment. On July 15, 2020, without foundational cybersecurity controls in place, HHS directed hospitals to report their COVID-19 data to TeleTracking. As of March 3, 2021, foundational controls were still not in place.

As with HHS Protect, the foundational cybersecurity controls were not implemented because OCIO management prioritized operational needs over completing the required processes for identifying, implementing, and testing cybersecurity controls. Instead, OCIO performed ad hoc

testing prior to allowing the TeleTracking system to collect COVID-19 hospital data and did not document the testing methods or results. The Federal Information Security Modernization Act of 2014 (FISMA), Section 3554 requires that Federal information systems meet the minimum information security system requirements described under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3). As a result, TeleTracking and the public health data it contains have an increased risk for unauthorized disclosure, alteration, and destruction, as well as cyberattack.

Appendix C contains further details on our analysis of TeleTracking cybersecurity documentation.

HHS DID NOT HAVE A PROCESS FOR ENSURING CYBERSECURITY OF RAPIDLY DEVELOPED SYSTEMS

The public health crisis caused by the COVID-19 pandemic presented unprecedented challenges. To respond to the challenges, OCIO was asked to rapidly deploy systems to collect and report critical data from States, communities, and hospitals to be used in the Federal response to the COVID-19 pandemic. It did so by deploying HHS Protect, including TeleTracking, for operational use less than 2 months after WHO declared COVID-19 to be a pandemic.

However, OCIO did not take steps to ensure that cybersecurity risks were mitigated prior to deploying these systems. This occurred because HHS management officials prioritized the mission to combat the COVID-19 pandemic over Federal requirements for developing, assessing, and authorizing a Federal IT system to officially operate prior to deploying HHS Protect and TeleTracking. Additionally, HHS did not have a documented and approved, streamlined version of the traditional assessment and authorization process that could be used to rapidly deploy an IT system. Such a process would assist HHS in rapidly deploying mission critical systems while also ensuring some cybersecurity risks can be addressed before deployment. For example, the process could define the minimum tasks required to be completed, including implementation and testing of foundational cybersecurity controls, prior to a system's deployment to ensure the confidentiality, integrity, and availability of the system and its data.

Federal guidance requires that leaders and managers identify, assess, and respond to risks from external and internal sources.⁷ However, there is no requirement that Federal agencies establish a process for rapidly deploying systems. OIG recognizes that the HHS mission may necessitate that it be prepared to respond to challenges from unique public health emergencies and that Federal regulations empower senior officials to make risk-based decisions. Given the likelihood that HHS will be called upon to respond to future public health emergencies, developing a streamlined process to rapidly develop, assess, formally authorize, and deploy an IT system with the required foundational cybersecurity controls will better prepare HHS to respond to such emergencies and thwart potential IT disruptions and cyber threats.

The rollout of HHS Protect and TeleTracking demonstrated the need for HHS to improve its process for assessing and formally authorizing an IT system to operate. HHS will continue to play an important role in modernizing public health data and related infrastructure and in responding to public health emergencies. As those efforts continue, ensuring that cybersecurity controls are properly implemented and assessed in IT systems authorized to operate for official use will be critical to preventing, detecting, and recovering from cybersecurity incidents.

RECOMMENDATIONS

We recommend that the Department of Health and Human Services:

- reperform the security categorization of HHS Protect to factor in PII and update cybersecurity controls if necessary;
- complete implementation and testing of required cybersecurity controls for the HHS Protect system based on the appropriate security categorization, including the risk assessment and IT contingency plan;
- complete implementation and testing of required cybersecurity controls for the TeleTracking system based on the appropriate security categorization; and
- develop a streamlined process to identify, implement, and test cybersecurity controls for new IT systems that are rapidly deployed to meet a mission-critical need. The process should define the minimum set of critical security controls that must be implemented and tested prior to the system being authorized to operate and adhere to

⁷ Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*.

Federal cybersecurity requirements to complete the full process within a specific time period following deployment.

HHS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, HHS concurred with our fourth recommendation but did not concur with our first three recommendations. Regarding the fourth recommendation, HHS stated that it developed and implemented *OS Guidance for Emergency Response Authorization for IT Resources*, which was approved and signed by the HHS Chief Information Officer and Chief Information Security Officer on February 8, 2021. HHS also indicated that it will review, identify any gaps in, and update the guidance as necessary. We are encouraged by HHS's response to this recommendation, and we look forward to receiving and reviewing the supporting documentation as part of our audit followup process.

Listed below is a summary of HHS's comments and our responses. HHS also provided technical comments which we addressed, as appropriate. HHS's comments are included in their entirety in Appendix D.

REPERFORM THE SECURITY CATEGORIZATION OF HHS PROTECT

HHS Comments

HHS stated that the Privacy Impact Assessment for HHS Protect was accurate regarding the presence of PII and the categorization of moderate for the system was correct even with the presence of PII; therefore, no additional system categorization was needed.

OIG Response

Our concerns were not primarily focused on the accuracy of the categorization, but that HHS did not provide support that cybersecurity testing considered the presence of PII when controls were designed and implemented. HHS did not support that the categorization and cybersecurity testing were performed with the awareness that HHS Protect contained PII. We agree with HHS that the PIA included recognition that HHS Protect had PII. However, supporting documentation provided by HHS did not consistently identify that HHS Protect stored PII. Although additional assessment may not change the security categorization of moderate, if steps that supported the assessment were conducted without awareness that HHS Protect contained PII, the design and implementation of controls may not be sufficient to protect PII. Therefore, we maintain that this recommendation and its related findings are valid.

ENSURE CYBERSECURITY OF HHS PROTECT AND TELETRACKING

HHS Comments

For our second and third recommendations, HHS stated that it had performed the necessary steps to ensure the cybersecurity of HHS Protect and TeleTracking including selection of FedRAMP approved products. For TeleTracking, HHS stated that it “was satisfied with the level of documentation provided by TeleTracking and continues to work through the process of obtaining a full ATO.”

OIG Response

Using a cloud service offering (CSO) that is listed as FedRAMP authorized provides some level of assurance, but it does not fulfill the federal ATO requirement. The “FedRAMP authorized” designation indicates that FedRAMP requirements are being met and a CSO’s security package is available for agency reuse. Agencies reusing a CSO can request access to that CSO’s security package from FedRAMP in order to review the package. Agencies still must issue their own ATO for the CSO. As part of the ATO, agencies must identify and address new risks that result from combining FedRAMP authorized CSOs with the user’s environment and configurations. HHS has stated that it reviewed the security package for TeleTracking and for the technologies used in HHS Protect. HHS did not provide documentation to support reviews of the security packages or that it had considered potential risks resulting from combining or using FedRAMP authorized CSOs in the HHS Protect environment and current configurations.

HHS Protect and TeleTracking were both launched prior to completion of an ATO and documentation of federally mandated cybersecurity testing. Both systems remain in production but do not comply with Federal requirements as of March 3, 2021 when HHS last provided documentation for this report. HHS Protect does not have a risk assessment and an IT contingency plan. TeleTracking is still in operation without an ATO and without documented completion of cybersecurity testing. Therefore, we maintain that these recommendations and their related findings are valid.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed HHS's procedures and IT security documentation provided by HHS related to HHS Protect and TeleTracking to determine whether foundational cybersecurity controls were in place and tested as well as verified in compliance with NIST guidance. We also interviewed HHS personnel. We conducted our audit work from August 2020 through May 2021.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal regulations and guidance including FISMA, OMB circulars, and NIST SPs and standards;
- obtained and reviewed HHS's existing IT system policies, procedures, practices, and security documentation;
- reviewed HHS Protect and TeleTracking IT security documentation to include the system control baseline, system security plan, access controls, contingency planning, risk and privacy impact assessments, vulnerability assessments, and authorization to operate memos;
- observed HHS personnel accessing and demonstrating some HHS Protect features;
- obtained authorized user access to HHS Protect to test some user access controls;
- interviewed HHS officials; and
- discussed our findings with HHS 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: FEDERAL REQUIREMENTS AND GUIDANCE

Federal Information Processing Standards

Publication 199: Standards for Security Categorization of Federal Information and Information Systems

Security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Publication 200: Minimum Security Requirements for Federal Information and Information Systems. These standards require that organizations:

1. determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
2. derive the information system impact level from the security category in accordance with FIPS 200; and
3. apply the appropriately tailored set of baseline security controls in NIST SP 800-53, R4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Federal Information Security Modernization Act of 2014

Section 3554

Agencies must comply with the policies, procedures, standards, and guidelines promulgated under the Act's section 11331 of title 40, which requires that Federal information systems meet the minimum information security system requirements described under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

National Institute of Standards and Technology Special Publications

NIST SP 800-34, Revision 1 - Contingency Planning Guide for Federal Information Systems. The guide requires that:

HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls (A-18-20-06800) 15

Warning—This report contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. § 522). If disclosed, the information in this report could adversely affect information security on U.S. Government Systems. Distribution should be strictly limited. Do not reproduce or release to any person without prior approval from the Department of Health and Human Services, Office of Inspector General, Office of Audit Services.

1. an organization develops contingency plans for each information system to meet the needs of critical system operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal contingency plan by the information system contingency plan coordinator, and must be reviewed annually and updated as necessary by the coordinator;
2. an organization conducts a system business impact analysis that includes the following steps:
 - a. determines mission or business processes and recovery criticality,
 - b. identifies resource requirements, and
 - c. identifies recovery priorities for system resources;
3. moderate-impact systems have functional exercises that include a simulated disruption with a system recovery component such as backup tape restoration or server recovery. High-impact systems should have full-scale functional exercises to include simulation prompting a full recovery and reconstituting the information system to a known state, and that ensures staff are familiar with the alternate facility.

NIST SP 800-37, Revision 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

This guidance does not provide for a “conditional” ATO. It permits an authorizing official to “authorize the system to operate only for a short period of time if it is necessary to test a system in the operational environment before all controls are fully in place” A risk assessment is still a prerequisite for issuing an ATO with a short operating period. (See the publication’s Appendix F, page 143.)

NIST SP 800-39 - Managing Information Security Risk, Chapter 2.1 states that the purpose of a risk assessment component is to identify:

1. threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;
2. vulnerabilities internal and external to organizations;

3. harm (i.e., consequences and/or impact) to organizations that may occur given the potential for threats that exploit vulnerabilities; and
4. the likelihood that harm will occur.

The result of an assessment is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).

NIST SP 800-53, Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations. This covers the recommended security controls and associated assessment procedures for Federal information systems and organizations. Security controls are listed by control family. Control families include but are not limited to:

- access control,
- configuration management,
- contingency planning,
- identification and authentication,
- incident response,
- personnel security,
- planning,
- risk assessment,
- security assessment and authorization,
- system and communications protection, and
- system and information integrity.

Agencies are required to have written policies and procedures for the minimum-security controls, which are determined by the impact baseline of the information system.

Office of Management and Budget Circulars

No. A-123 – Management’s Responsibility for Internal Control

This circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. The circular includes an attachment that defines management’s responsibilities related to internal control and the process for assessing internal control effectiveness.

No. A-130, Appendix III – Security of Federal Automated Information Resources

Section A(3)(b)(4) requires that Federal agencies ensure that a management official authorizes in writing the use of the application by confirming that its security plan as implemented adequately secures the application. Results from the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least once every 3 years thereafter. Management authorization implies accepting the risk attached to each system used by the application.

APPENDIX C: SECURITY DOCUMENT REVIEW TABLE

HHS Protect Security Documents

IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
1	Designation memos for security officer and information systems security officer	8/12/2020	Received 9/8/2020	Memos contained required signatures.
2	System security plans, including Appendix X (with control implementations)	8/12/2020	Received 1/6/2021	A system security plan includes a network diagram, points of contact, system categorization, and high-level information on how the system is protected. HHS completed all 261 NIST-required controls for a “moderate” system and completed 18 additional controls.
3	Risk assessments	8/12/2020	No	No system risk assessments. Without an assessment, there is no assurance HHS has assessed the risk to confidentiality, integrity, and availability of HHS Protect.
4	PIA/Privacy threshold analysis	8/12/2020	Received 12/10/2020 and 1/6/2021 (additional comments added after 12/10/2020)	The PIA indicated that PII for “above 2,000” individuals is maintained in the system. The official website and HHS officials stated that the system did not contain PII and/or PHI.
5	FIPS Publication 199 rating	8/12/2020	Received 12/10/2020	HHS Protect was deemed “moderate” both overall and in terms of confidentiality, integrity, and availability.
6	Contingency plan and test results	8/12/2020	No	No contingency plan. Without an approved contingency plan, there is no assurance the system can recover in the event of a disaster, whether man-made (such as hacking) or natural.
7	Incident response plan	8/12/2020	Received 1/6/2021	The incident response plan provided details on response contacts, categorizing incident types, how to prioritize incidents, and general handling procedures.

IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
8	Interconnection Security Agreement (ISA)/Memorandum of Understanding	8/12/2020	Received 1/6/2020	The ISA documents the security agreement between CDC and HHS. The document includes encryption level requirements and security-related responsibilities for both CDC and HHS. Note: The ISA states that CDC collects PII, and that data will be passed between CDC and HHS.
9	Security assessment report (SAR)	8/12/2020	Received 1/6/2021	Vulnerabilities reported as part of the SAR included one critical, one high, four medium, and one low severity vulnerabilities. The SAR included remediation recommendations.
10	Third-party assessments	8/12/2020	No	No third-party assessments were conducted on HHS Protect. Without third-party assessments, there is no assurance that the HHS Protect platform has been independently assessed for security risks.
11	Plan of Action and Milestones (POA&Ms)	8/12/2020	Received 1/20/2021	POA&Ms included four medium severity and one low severity vulnerabilities and were expected to be completed in March and April 2021, respectively. Note: The ATO stated that critical and high vulnerabilities were remediated.
12	E-authentication risk assessment (RA)	8/12/2020	Received 1/6/2021	The e-authentication RA shows minimum security is a single-factor authentication. HHS is using multifactor. Note: HHS selected "yes" in response to the question, "Are you making PII or PHI accessible?" This statement contradicts HHS's statement that there is neither PII nor PHI in HHS Protect.
13	ATO letter and/or memo	8/12/2020	Received 1/20/2021	The system was operational on 4/10/2020. A conditional ATO was not approved until 8/18/2020, so the system was operating without any type of ATO for approximately 4 months. A formal ATO was approved on 1/19/2021.

TeleTracking Security Documents

IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
1	System security plan	8/12/2020	No	No system security plan. Without a system security plan, there is no assurance of adequate security protection for the system.
2	Security scans	8/12/2020	Received 10/8/2020	Security scans showed a minimal number of weaknesses and/or flaws. One scan resulted in an overall score of 99 out of 100, another showed a 0 risk score and 0 vulnerabilities, and an enterprise penetration test resulted in findings of one high, two moderate, and one low. These scans/tests provided some assurance that potential risks and flaws in TeleTracking had been assessed and addressed.
3	TeleTracking policy manuals	8/12/2020	Received 10/8/2020	Policy manual topics included training and awareness, a statement of applicability, an information security policy, and the Information System Management Security scope.
4	International Organization for Standardization (ISO) certification	8/12/2020	Received 10/8/2020	TeleTracking was certified by the SRI Quality System Registrar with respect to the requirements of ISO/IEC 27001:2013 (i.e., international level Information security framework).
5	Third-party assessment	8/12/2020	Received 10/8/2020	The third-party assessment documentation included intelligence gathering, threat modeling, penetration testing, vulnerability analysis, and exploitation. The assessment resulted in one high, two moderate, and one low finding and/or weakness.
6	Interconnection Security Agreement (ISA)	8/12/2020	Received 10/8/2020	The agreement documents the interconnection security agreement between CDC and HHS. This document includes encryption level requirements and security-related responsibilities for both CDC and HHS. Note: The ISA states CDC collects PII and that data will be passed between CDC and HHS.
7	Risk assessments	8/12/2020	No	No system risk assessments. Without the assessment, there is no assurance HHS has assessed the risk to the confidentiality, integrity, and availability of TeleTracking.

IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
8	ATO letter and/or memo	8/12/2020	No	HHS did not complete an ATO for TeleTracking even though TeleTracking had been in operation since July 13, 2020. Without an ATO, there is no assurance that risks to organizational operations have been properly assessed and that management has explicitly accepted the risks.

APPENDIX D: HHS COMMENTS



OFFICE OF THE CHIEF INFORMATION OFFICER DEPARTMENT OF HEALTH AND HUMAN SERVICES

August 31, 2021

To: Christi A. Grimm
Principal Deputy Inspector General

From: Janet Vogel
Acting Chief Information Officer

Subject: Response to OIG Draft Report: *HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls*, A-18-20-06800

Thank you for the opportunity to review and comment on the Office of the Inspector General (OIG) Draft Report entitled, *HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls* (A-18-20-06800). We appreciate the partnership between the OIG and OCIO as we strive to best protect HHS's information systems and the information with which we are entrusted.

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 information technology security 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 HHS Acting Chief Information Security Officer, Christopher Bollerer at Christopher.Bollerer@hhs.gov or (202) 774-2121.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the *Review of the Draft Report entitled, HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Control, (A-18-20-06800)*

cc:

Christopher Bollerer, HHS Acting Chief Information Security Officer
Jeffrey Arman, Assistant Director, OIG Cybersecurity & IT Audit Division

US Department of Health and Human Services
Office of the Chief Information Officer (OCIO) /Office of Information Security (OIS)

HHS Protect and TeleTracking Were Launched Without Foundational Cybersecurity Controls (A-18-20-06800) 23

Warning—This report contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. § 522). If disclosed, the information in this report could adversely affect information security on U.S. Government Systems. Distribution should be strictly limited. Do not reproduce or release to any person without prior approval from the Department of Health and Human Services, Office of Inspector General, Office of Audit Services.



August 2021

Attachment A: OCIO Response to the Draft Report “HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls” (A-18-20-06800)

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) appreciates the long-standing partnership with the Office of Inspector General (OIG). The OIG provides a necessary, independent and vital source of information and insight that directly benefits HHS’s cybersecurity program and the protection of the data with which HHS is entrusted. HHS OCIO offers the following response to the OIG’s recommendations contained within the draft report entitled *HHS Protect and TeleTracking were Launched Without Foundational Cybersecurity Controls* (A-18-20-06800).

During this unprecedented time, HHS’s resources are focused on the fight against the COVID-19 pandemic. In support of this effort, and in response to various legislative mandates and other requirements¹, OCIO and OIS were charged with the immediate implementation of systems and technologies to aid pandemic response. The Department identified and evaluated the most effective technologies and quickly deployed them in the form of HHS Protect, a critical component of HHS’s response.

HHS Protect is a secure platform for authentication, amalgamation and sharing of healthcare information, enabling the Federal government to harness the power of data to inform its COVID-19 response. HHS Protect unifies more than 200 disparate healthcare data sources into one ecosystem that integrates data across federal, state and local governments as well as the Healthcare and Public Health (HPH) sector. As a result, HHS Protect provides a holistic view of the U.S. healthcare system, ensuring that decision-makers are well-informed and are equipped to guide action and save lives with data-driven COVID-19 response efforts.

While, as stated in the conditional Authorization to Operate (ATO) the OIG team reviewed, HHS did not initially perform all activities normally associated with the ATO process, HHS deployed these technologies only after careful review and evaluation. OCIO personnel reviewed comprehensive, security-focused documentation and met with vendor personnel to understand in-place cybersecurity controls as well as risks that may be present in those technologies. In addition, the vast majority of the tools and technologies comprising the HHS Protect system are cloud-based and authorized for federal use through the Federal Risk and Authorization Management Program (FedRAMP). Leveraging FedRAMP authorized systems ensures that these technologies have been thoroughly documented and tested, are authorized for federal use, and are continuously monitored for risks and vulnerabilities. Using FedRAMP authorized systems minimizes the number of security controls for which HHS is responsible; HHS must document, test and implement only hybrid and customer-specific security controls, as delineated

¹ Legislation and other requirements include but are not limited to the CARES Act (Coronavirus Aid, Relief, and Economic Security Act), H.R. 748, Enacted March 27, 2020; Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020, H.R. 6074, Public Law 116-123, Enacted March 4, 2020; President’s Designation of Emergency Requirements in accordance with H.R. 6074, published as H. Doc. 116-106, March 9, 2020; and Presidential Proclamation 9994 of March 13, 2020 Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak (as printed in the Federal Register, March 18, 2020, 85 FR 15337).



August 2021

Attachment A: OCIO Response to the Draft Report “HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls” (A-18-20-06800)

in FedRAMP authorization packages. This means that HHS was able to quickly implement the HHS Protect system with confidence that most security controls associated with the system were appropriately configured, documented, tested and regularly monitored.

Recommendation #1: Reperform the security categorization of the HHS Protect system in accordance with NIST FIPS Publication 199 to factor in PII as noted in the PIA and update cybersecurity controls as necessary.

HHS Response: Non-Concur

HHS provided revised security documentation and other artifacts for HHS Protect while audit fieldwork was being conducted. This documentation included a revised FIPS 199 categorization. The FIPS 199 categorization document combined with the Privacy Impact Assessment (PIA) – a mandatory component of all HHS ATO packages – included an accurate, up-to-date characterization of the PII contained within the HHS Protect system. The acknowledgement that HHS Protect contains PII did not, however, necessitate any change to the overall FIPS 199 categorization of *moderate*.

Recommendation #2: Immediately complete implementation and testing of foundational cybersecurity controls for HHS Protect system based on the appropriate security categorization including the risk assessment and contingency plan.

HHS Response: Non-Concur

As noted in the conditional ATO reviewed by the OIG, HHS immediately implemented a traditional ATO process upon selection of the appropriate platform. A risk-based approach was taken that considered data sensitivity, exposure, threat and impact to HHS’s COVID-19 response efforts. This included ensuring the security and privacy of systems supporting information and data related to the response. HHS Protect, specifically, was thoroughly interrogated by penetration testing activities and web-application scans. Furthermore, HHS ensured the Software as a Service (SaaS) Palantir platform was secured to meet FedRAMP security standards and the agency level controls were applied to meet least-privilege control settings. These activities include the testing of all security controls for which HHS is responsible, and the development of required documentation such as a contingency plan, system security plan and risk assessment.

In standing up the HHS Protect system, the HHS team sought to leverage cloud-based technologies with valid FedRAMP authorizations. This ensured that HHS used proven, secure technologies authorized for use by the federal government while minimizing the number of security controls HHS was required to implement and test. The Palantir platform – the foundation on which HHS Protect is built – is a moderate system with 262 security controls



August 2021

Attachment A: OCIO Response to the Draft Report “HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls” (A-18-20-06800)

required for implementation. Of those 262 controls, HHS has the responsibility to document, implement and test approximately 27. The remaining controls are directly inherited from the FedRAMP authorization. That is a considerable reduction in the work HHS must do to authorize the system and means that nearly 90% of the security controls were proven to be operating effectively regardless of the status of HHS’s ATO documentation. HHS had confidence in the underlying platform’s security controls which allowed HHS to quickly stand up HHS Protect and address remaining security controls while simultaneously addressing the immediate requirement to establish a data aggregation platform supporting the fight against COVID-19.

Furthermore, HHS performed web application scans, ensured 3rd party penetration testing activity and ensured all critical, high and moderate findings were remediated before allowing the system to be authorized. HHS implemented and maintains full controls of secure multifactor authentication access to HHS Protect. HHS reviews monthly scan results for HHS Protect to ensure the system is meeting continuous monitoring controls and requirements.

Moreover, HHS acted as the FedRAMP sponsor for the Palantir platform used as the foundation for HHS Protect. HHS’s sponsorship role saw the OCIO team shepherding Palantir through the rigorous FedRAMP authorization process, comprehensively reviewing all FedRAMP authorization documentation² and results of in-depth independent third-party testing. Through this sponsorship activity, HHS oversaw the development of a complete and comprehensive FedRAMP compliant ATO package, gained insight into the risks identified by testing, and understood the processes Palantir used to remediate those risks. The HHS team continues to meet with Palantir on a monthly basis, meeting FedRAMP requirements to monitor the system on a continuous basis. As such, HHS has continuous insight into the security controls employed to protect the Palantir platform, ensuring that the system remains secure consistent with the FedRAMP authorization HHS granted.

Recommendation #3: Immediately complete implementation and testing of foundational cybersecurity controls for TeleTracking system based on the appropriate security categorization.

² Per FedRAMP requirements, this package includes but is not limited to the following documents: System Security Plan (including the attachments Information Security Policies and Procedures, User Guide, Digital Identity Worksheet, Privacy Threshold Analysis, Privacy Impact Analysis, Rules of Behavior, Information System Contingency Plan, Configuration Management Plan, Incident Response Plan, Control Implementation Summary Workbook, Federal Information Processing Standards 199, Separation of Duties Matrix, Integrated Inventory Workbook), the Security Assessment Plan (including Security Test Case Procedures, Penetration Testing Plan and Methodology, and 3PAO Supplied Deliverables), the Security Assessment Report (including the appendices Risk Exposure Table, Security Test Case Procedures, Infrastructure Scan Results, Database Scan Results, Web Scan Results, Auxiliary Documents, and Penetration Test Report), the Plan of Action and Milestones to include the Continuous Monitoring Strategy and Continuous Monitoring Monthly Executive Summary) and the FedRAMP ATO letter.



August 2021

Attachment A: OCIO Response to the Draft Report “HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls” (A-18-20-06800)

HHS Response: Non-Concur

TeleTracking was selected by HHS leadership as a leader in healthcare data collection, specifically in relation to hospital data. At the start of COVID-19, TeleTracking was awarded a contract to immediately begin collection of hospital capacity data so that the Office of the Assistant Secretary for Preparedness and Response (ASPR) had all of the necessary information to respond accordingly to the pandemic. ASPR requested support of HHS OCIO to help implement this capability and integrate with existing COVID-19 response systems. At that time, HHS OCIO viewed TeleTracking as a data source that fed hospital data into HHS Protect. However, as mission requirements evolved, the capabilities of TeleTracking expanded and HHS OCIO recognized that the system needed to be categorized as a FISMA system. OCIO continued to engage TeleTracking and collected security documentation to move the system through the ATO process. In standing up TeleTracking, the HHS team sought to leverage an existing commercial off-the-shelf (COTS) solution meeting Health Insurance Portability and Accountability Act (HIPAA) and other relevant industry requirements. This ensured that HHS used proven, secure technologies while minimizing the number of security controls HHS was required to implement and test. The TeleTracking platform is a moderate system with numerous security controls in place. HHS was satisfied with the level of documentation provided by TeleTracking and continues to work through the process of obtaining a full ATO. HHS ASPR and OCIO launched the TeleTracking reporting environment while simultaneously addressing the immediate requirement to establish a data aggregation platform supporting the fight against COVID-19.

Furthermore, HHS performed web application scans, ensured 3rd party penetration testing activity and ensured all critical, high and moderate findings were remediated before allowing the system to be authorized.

Recommendation #4: Develop a streamlined approach for authorizing the operation of a new IT system that is being rapidly deployed to meet a mission critical need. The approach should define the minimum set of critical security controls that must be implemented and tested prior to the system being authorized to operate and adhere to Federal cybersecurity requirements to complete the full process within a specific time after deployment.

HHS Response: Concur

During the course of the OIG’s audit work, leveraging the feedback provided throughout the engagement, OIS developed and implemented *OS Guidance for Emergency Response Authorization (ERA) for IT Resources*, approved and signed by the HHS Chief Information Officer and Chief Information Security Officer on February 8, 2021. This guidance:

- Establishes specific criteria under which emergency authorizations can be conducted;



August 2021

Attachment A: OCIO Response to the Draft Report “HHS Protect and TeleTracking were launched Without Foundational Cybersecurity Controls” (A-18-20-06800)

- Provides guidance for expedited system authorizations including requirements for testing, vulnerability scanning, patching, and vulnerability monitoring, remediation and reporting;
- Establishes specific roles and responsibilities for the authorizing official, business owners, system owners, information system security officers, system administrators and system users;
- Delineates the documentation and actions necessary for obtaining an ERA; and
- Identifies post-authorization requirements and actions.

We believe this guidance satisfies much of the OIG’s recommendation; we will review, identify any gaps, and update the guidance as necessary.