Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HHS Did Not Ensure Foundational Cybersecurity Controls Were In Place Prior To Implementation Of HHS Protect And Use of a Contractor's Cloud Service

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

December 2023
A-18-20-06800R

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

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. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, 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: December 2023
Report No. A-18-20-06800R

U.S. Department of Health & Human Services
Office of Inspector General

HHS Did Not Ensure Foundational Cybersecurity Controls Were in Place Prior to Implementation of HHS Protect and Use of a Contractor's Cloud Service

Why OIG Did This Audit

HHS deployed Protect.HHS.gov (HHS Protect) to collect and report critical data from States, communities, and hospitals to be used in the Federal response to the COVID-19 pandemic. Ensuring that systems such as HHS Protect that support the COVID 19 response have implemented foundational cybersecurity controls is important to ensuring the integrity and availability of critical public health data.

Our objective was to determine whether HHS implemented foundational cybersecurity controls in order to ensure the integrity and availability of HHS Protect and the U.S. Healthcare COVID-19 Portal.

How OIG Did This Audit

We focused on determining whether HHS ensured the implementation of cybersecurity controls that are foundational to securing HHS Protect and the U.S. Healthcare COVID-19 Portal prior to their official use. We requested and reviewed HHS's documentation that described the cybersecurity controls in place to ensure the integrity and availability of HHS Protect and the U.S. Healthcare COVID-19 Portal.

On August 24, 2022, we rescinded the report because 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 originally issued report) was inaccurate based on information and documentation obtained after completion of the audit. We performed additional audit work, revised the report, and are reissuing the report under number A-18-20-06800R.

What OIG Found

HHS did not ensure that select cybersecurity controls, which are foundational to the integrity and availability of an information system and its data, were in place prior to the launch of HHS Protect. Specifically, HHS had not completed a privacy impact assessment, risk assessment, security categorization process, system security plan, and contingency plan. Additionally, HHS had not completed the Federal Risk and Authorization Management Program (FedRAMP) security assessment and authorization tasks for its contractor's cloud service that provided HHS access to and use of hospital data collected via the U.S. Healthcare COVID-19 Portal. HHS was responsible for performing the FedRAMP security assessment and authorization tasks to confirm that the federally required foundational cybersecurity controls had been implemented and were operating effectively prior to using hospital data received via the portal.

HHS relied on HHS Protect and the U.S. Healthcare COVID-19 Portal to provide critical information for pandemic decision-making without determining whether the systems and data were susceptible to an unacceptably high risk of failure or compromise from unintentional disruptions (e.g., man-made or natural disasters) or intentional disruptions such as cyberattacks.

What OIG Recommends

The rescinded report included four recommendations. HHS concurred with one of the four recommendations and did not concur with the other three recommendations. Based on the additional work performed, the finding in the report regarding the U.S. Healthcare COVID-19 Portal was revised. Our additional audit work revealed that HHS did not complete the FedRAMP security assessment and authorization tasks for its contractor's cloud service. The contractor, a cloud service provider (CSP), granted HHS access to and use of hospital data that was being collected via the U.S. Healthcare COVID-19 Portal. HHS was responsible for ensuring that the FedRAMP tasks were performed for the cloud service prior to receiving the hospital data the CSP was collecting to confirm that the federally required foundational cybersecurity controls had been implemented and had been operating effectively. HHS relied on COVID-19 hospital data provided by a CSP without confirming that the security controls were in place and operating effectively to ensure the integrity and availability of the data. Instead of revising the

The full report can be found at https://oig.hhs.gov/oas/reports/region18/A182006800R.asp.

recommendation, we removed it because the HHS Office of the Chief Information Officer informed us that it no longer had a contract for the cloud service and the U.S. Healthcare COVID-19 Portal was no longer in use. The three remaining recommendations are listed below.

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

Based on our additional work, we are closing all three recommendations. We are closing the first two recommendations because HHS transferred HHS Protect to the Centers for Disease Control and Prevention. We are closing the third recommendation based on HHS's development of the *OS Guidance for Emergency Response Authorization (ERA) for IT Resources,* which defines 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 following deployment.

TABLE OF CONTENTS

APPENDICES

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS) deployed Protect.HHS.gov (HHS Protect) to collect and report critical data from States, communities, and hospitals to be used in the Federal response to the COVID-19 pandemic. HHS gave hospitals four options to submit COVID-19 data to HHS, including via the U.S. Healthcare COVID-19 Portal. HHS Protect 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 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

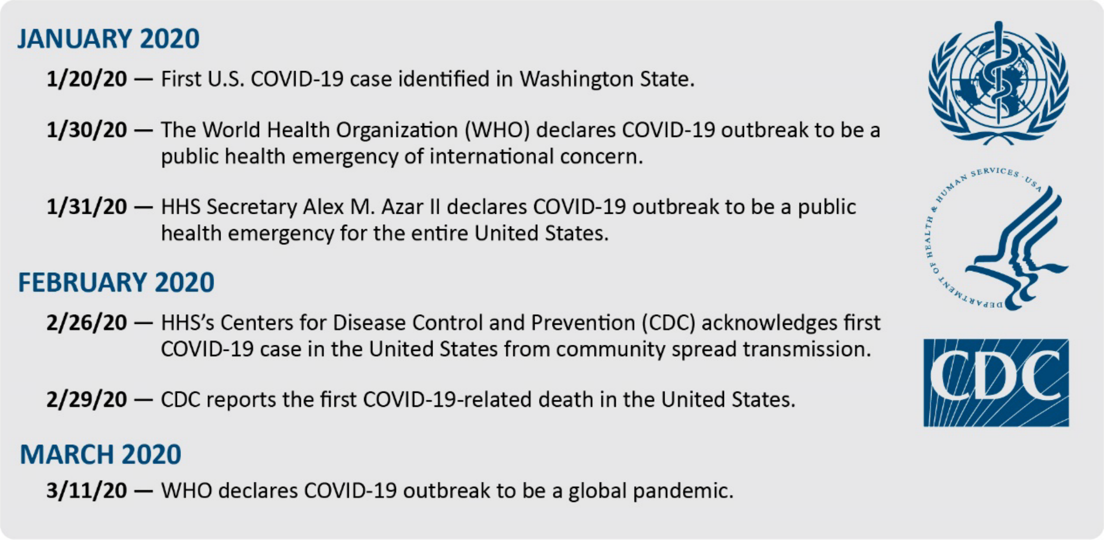
Our objective was to determine whether HHS implemented foundational cybersecurity controls in order to ensure the integrity and availability of HHS Protect and the U.S. Healthcare COVID-19 Portal.

[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

Initial Progression of COVID-19 in the United States



JANUARY 2020

1/20/20 — First U.S. COVID-19 case identified in Washington State.

1/30/20 — The World Health Organization (WHO) declares COVID-19 outbreak to be a public health emergency of international concern.

1/31/20 — HHS Secretary Alex M. Azar II declares COVID-19 outbreak to be a public health emergency for the entire United States.

FEBRUARY 2020

2/26/20 — HHS's Centers for Disease Control and Prevention (CDC) acknowledges first COVID-19 case in the United States from community spread transmission.

2/29/20 — CDC reports the first COVID-19-related death in the United States.

MARCH 2020

3/11/20 — WHO declares COVID-19 outbreak to be a global pandemic.

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 (IT) infrastructure across the agency. Operating divisions (OpDivs) and staff divisions (StaffDivs) involved in the COVID-19 pandemic response include the Office of the Administration for Strategic Preparedness and Response (ASPR),[3] 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. Available online at https://www.fema.gov/sites/default/files/2020-07/fema_ESF_8_Public-Health-Medical.pdf. Accessed on June 3, 2021.

[3] ASPR was formerly known as the Office of the Assistant Secretary for Preparedness and Response. In July 2022, the office was elevated from a staff division to an operating division and renamed the Administration for Strategic Preparedness and Response.

and was burdensome for health care providers and others involved in direct public health response efforts. 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] 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.

U.S. Healthcare COVID-19 Portal

In April 2020, ASPR awarded a 6-month contract that provided HHS with access to and use of real-time hospital capacity data related to the COVID-19 pandemic. The contractor used the U.S. Healthcare COVID-19 Portal to aid in the collection of this hospital data and its existing software as a service-based commercial analytics platform to provide the hospital data to HHS.[6]

[4] Coronavirus Aid, Relief, and Economic Security (CARES) Act, P.L. No. 116-136 (Mar. 27, 2020); American Rescue Plan Act of 2021, P.L. 117-2 (Mar. 11, 2021).

[5] EO 13994, "Executive Order on Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats," Jan. 21, 2021. Available online 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/. Accessed on June 3, 2021.

[6] Software as a Service is a cloud service model whereby a consumer is provided the capability to use a provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

According to HHS officials, the contracted cloud service enabled HHS to streamline hospital data collection, quickly create new data fields, and collect nationwide data within 3 days. On July 15, 2020, at the direction of HHS, hospitals began to input requested COVID-19 data into the U.S. Healthcare COVID-19 Portal, if they were not already, or via their respective State health departments instead of submitting to CDC's National Healthcare Safety Network to reduce confusion and reporting duplication. The contract was extended in October 2020 for 6 months. In March 2021, OCIO awarded the contractor another 6-month contract to continue its work with HHS for the period from April through September 2021.

HOW WE CONDUCTED THIS AUDIT

We focused on determining whether HHS ensured the implementation of cybersecurity controls that are foundational to securing HHS Protect and the U.S. Healthcare COVID-19 Portal prior to their official use. To accomplish our objective, we requested and reviewed HHS's documentation that described the cybersecurity controls in place to ensure the integrity and availability of HHS Protect and the U.S. Healthcare COVID-19 Portal. We also interviewed HHS personnel and observed certain system cybersecurity controls in use during a demonstration of HHS Protect's capabilities.

We assessed whether HHS complied 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,* NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, and *HHS Memorandum: HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance*. The HHS memorandum includes the policy that OpDivs are required to comply with when acquiring and/or utilizing cloud services.

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.
- 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 HHS had implemented or ensured the implementation of the foundational cybersecurity controls that ensure the integrity and availability of HHS Protect and the U.S. Healthcare COVID-19 Portal, in accordance with Federal requirements. Our audit was not an assessment of all organizational internal or IT controls.

On August 24, 2022, we rescinded the report because 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 originally issued report) was inaccurate based on information and documentation obtained after completion of the audit. We have revised and are reissuing the report under number A-18-20-06800R. The revised report includes applying the appropriate criteria to HHS's use of a cloud service to provide access to and use of hospital data that was being collected via the U.S. Healthcare COVID-19 Portal. The report also incorporates information that was provided to the audit team subsequent to the publication of the original report and corrects errors.

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

HHS did not ensure that select cybersecurity controls, which are foundational to the integrity and availability of an information system and its data, were in place prior to the launch of HHS Protect. Specifically, HHS had not completed a privacy impact assessment (PIA), risk assessment, security categorization process, system security plan, or contingency plan. Although HHS issued a memo authorizing the operation of the system for official use with conditions, the memo acknowledged that all required IT security-related documentation along with other required IT security-related tasks had not been completed prior to the system's deployment.[7] HHS implemented three of the five foundational cybersecurity controls after HHS Protect was deployed. HHS granted HHS Protect an authorization to operate without conditions 9 months after its deployment on January 20, 2021. Additionally, HHS had not completed the Federal Risk and Authorization Management Program (FedRAMP) security assessment and authorization tasks for its contractor's cloud service that provided HHS access to and use of hospital data collected via the U.S. Healthcare COVID 19 Portal. HHS was responsible for performing the FedRAMP security assessment and authorization tasks to confirm that the federally required foundational cybersecurity controls had been implemented and were operating effectively prior to using hospital data received via the portal. Therefore, HHS was not in compliance with its own cloud-computing policy.

HHS relied on HHS Protect and the U.S. Healthcare COVID-19 Portal to provide critical information for pandemic decision-making without determining whether the systems and data were susceptible to an unacceptably high risk of failure or compromise from unintentional disruptions (e.g., man-made or natural disasters) or intentional disruptions such as cyberattacks. Although HHS had not reported a major incident for HHS Protect or the U.S. Healthcare COVID-19 Portal 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.

HHS did not ensure that foundational cybersecurity controls were implemented prior to the deployment of HHS Protect and the receipt and use of hospital data provided by HHS contractor's cloud service because HHS officials prioritized their operational use to achieve the agency's mission of combating the COVID-19 pandemic over meeting all the Federal requirements.

[7] The HHS Protect ATO memo with conditions documents the HHS authorizing official's decision to permit the system to operate in production for 120 days to allow time to complete the outstanding IT security-related tasks (e.g., risk assessment, contingency plan, and system security plan).

HHS DID NOT ENSURE REQUIRED CONTROLS WERE IMPLEMENTED PRIOR TO DEPLOYING HHS PROTECT

When HHS launched HHS Protect on April 10, 2020, it had not ensured that some foundational security controls were in place. Specifically, the PIA, security categorization, risk assessment, system security plan, and contingency plan had not been completed prior to the system's launch.[8] Additionally, HHS acknowledged in its April, August, and December 2020 written authorizations for the system to operate with conditions that it had not completed certain required actions. More specifically, HHS acknowledged that it did not complete required IT security documents and tasks prior to the system's deployment for operational use. OCIO officials explained that some ad hoc cyber assessments had been conducted 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 provided. On January 20, 2021, HHS provided a signed ATO memo without conditions. However, HHS did not provide a completed risk assessment or contingency plan for HHS Protect, which are required documents to support the authorization to operate without conditions, until nine months later in September 2021.

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 results of the PIA and system categorization process, HHS implemented security controls that it believed were adequate but may not have been sufficient or appropriate to ensure the integrity and availability of the system or its data.

Subsequent to our audit request for the PIA and categorization process documentation, HHS took action to complete both. A PIA is designed to identify privacy risks. The PIA results are published to inform the public if personal identifiable information (PII) is 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 memos signed on April 14, 2020, and August 19, 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 not selecting the appropriate cybersecurity controls for implementation. Absent or inadequate security controls expose the processing, storage, or

[8] HHS completed and provided the system security plan documentation during the audit.

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 Authorized HHS Protect to Operate Without Properly Verifying Cybersecurity

HHS launched HHS Protect on April 10, 2020, prior to completing the required tasks upon which an authorization to operate for official use should be based. The Office of Management and Budget (OMB) Circular No. A-130, *Appendix I: Responsibilities for Protecting and Managing Federal Information Resources*, Section 5(g) requires that a management official authorizes the use of the information system based on a review of the authorization package and includes an assessment of compliance with applicable requirements and risk.[9] HHS management made the decision not to complete the security plan and other required IT security tasks upon which an authorization to operate should be based because it prioritized making HHS Protect operational to combat the public health crisis. Without completing the required tasks that underpin the federally required authorization to operate, there is no assurance that HHS management has properly assessed the cybersecurity risks associated with HHS Protect, which puts public health data at increased risk for unauthorized disclosure or manipulation, as well as a cyberattack.

[9] Authorization package means the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

HHS signed an ATO memo with conditions on April 14, 2020, which was 4 days after HHS Protect was launched. The ATO memo acknowledged that a substantial amount of security-related documentation associated with the full security control assessment that would typically corroborate system security had not been completed. Some of the documentation that was supposed to be completed included the security assessment report, incident response plan, and corrective action plans for vulnerabilities identified, in addition to documentation related to the select foundational cybersecurity controls that we reviewed. The April 14, 2020, memo authorized the system to operate for 120 days (through August 12, 2020) to give HHS time to create all the security-related documentation associated with the full cybersecurity control assessment and perform other IT security tasks.

On August 19, 2020—7 days after the April 14, 2020, ATO memo expired—HHS signed a new memo authorizing the operation of the system for official use with conditions. The new memo was almost identical in its wording to the one signed April 14, 2020. The new memo was issued because HHS had not completed any of the outstanding security-related documentation associated with the full cybersecurity control assessment and performed the other IT security tasks within the 120 days that were noted in the April 14 memo. The August 19 memo authorized the system to operate with conditions for an additional 120 days (through December 17, 2020). On December 21, 2020, another 120-day extension was granted that again noted the lack of completed security-related documentation and other IT security tasks. On January 20, 2021, 9 months after the system was deployed, an ATO memo without conditions was signed that granted permission for HHS Protect to operate for official use.

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

HHS DID NOT COMPLY WITH HHS POLICY PRIOR TO USING A CLOUD SERVICE

HHS did not comply with its cloud computing policy prior to contracting with a cloud service provider (CSP) that operated the U.S. Healthcare COVID-19 Portal to obtain COVID-19 hospital data. At the time HHS began using the CSP's services, the CSP did not have a FedRAMP-compliant ATO and HHS did not perform the FedRAMP security assessment and authorization of the CSP. However, the HHS memorandum "HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance" states that HHS "is responsible for performing the FedRAMP security assessment and authorization" when the CSP does not have a FedRAMP compliant ATO.[10] The HHS memo also states that the HHS Chief Information Officer (CIO), or the CIO's designee, is the Authorizing Official responsible for granting an ATO for all HHS-sponsored CSPs. At the time, HHS officials prioritized the operational use of the cloud service to achieve the agency's mission of combating the COVID-19 pandemic over meeting the Federal

[10] FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

requirements to complete the security assessment and privacy documentation prior to authorizing a system to operate.

HHS relied on COVID-19 hospital data provided by the cloud service without confirming that the security controls were in place and operating effectively to ensure the integrity and availability of the data. HHS's contract for the cloud service ended on December 31, 2022, and the U.S. Healthcare COVID-19 Portal is no longer operational.

Appendix C contains further details on our analysis of the cybersecurity documentation related to the U.S. Healthcare COVID-19 Portal.

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, HHS needed a central way 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 for operational use less than 2 months after the World Health Organization declared COVID-19 to be a pandemic.

However, OCIO did not complete all required IT security-related assessments, tasks, and authorizations to ensure that cybersecurity risks were mitigated prior to launching HHS Protect. 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. 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 a new IT system. Such a process would assist HHS in rapidly deploying mission critical systems while also ensuring that some cybersecurity risks can be addressed before deployment. For example, the process could define the minimum number of 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.[11] 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.

[11] OMB Circular A-123, *Management's Responsibility for Internal Control*.

The findings of this report demonstrate the need for HHS to improve its process for assessing and formally authorizing IT services. 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.
- 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 Federal cybersecurity requirements to complete the full process within a specific time following deployment.

HHS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, which contained four recommendations, HHS concurred with one recommendation but did not concur with three recommendations. As noted earlier, we rescinded the report because 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 originally issued report) was inaccurate based on information and documentation obtained after completion of the audit.

Based on the additional work performed, the finding in the report regarding the U.S. Healthcare COVID-19 Portal was revised. Our additional audit work revealed that HHS did not complete the FedRAMP security assessment and authorization tasks for its contractor's cloud service. The contractor, a CSP, granted HHS access to and use of hospital data that was being collected via the U.S. Healthcare COVID 19 Portal. HHS was responsible for ensuring that the FedRAMP tasks were performed for the cloud service prior to receiving the hospital data the CSP was collecting to confirm that the federally required foundational cybersecurity controls had been implemented and had been operating effectively. HHS relied on COVID-19 hospital data provided by a CSP without confirming that the security controls were in place and operating effectively to ensure the integrity and availability of the data. Instead of revising the recommendation, we removed it because OCIO informed us that it no longer has a contract for the cloud service and the U.S. Healthcare COVID-19 Portal is no longer in use.

In addition, while completing additional work, HHS transferred HHS Protect to CDC. As a result, we are closing the following recommendations that HHS:

- reperform the security categorization of HHS Protect to factor in personal identifiable information and update cybersecurity controls, if necessary; and,
- 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.

We are also closing the recommendation that HHS 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 because OCIO has taken corrective action that addressed the recommendation. Specifically, we verified that HHS developed the *OS Guidance for Emergency Response Authorization (ERA) for IT Resources*, which defines 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 following deployment.

HHS's comments, excluding its technical comments, are included as Appendix D. HHS also provided technical comments to the report, which we addressed as appropriate.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed HHS's procedures and IT security documentation provided by HHS related to HHS Protect and the U.S. Healthcare COVID-19 Portal 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.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal regulations and guidance including the Federal Information Security Modernization Act, OMB circulars, and NIST SPs and standards;
- obtained and reviewed HHS's existing IT system policies, procedures, practices, and security documentation;
- reviewed HHS Protect IT security documentation and IT security documentation related to the contracted cloud service including 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;
- discussed our findings with HHS officials; and
- provided the revised report to HHS official for review and addressed technical comments, as appropriate.

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 (FIPS)

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 each organization:
>
> 1. determines the security category of its information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
>
> 2. derives the information system impact level from the security category in accordance with FIPS 200; and
>
> 3. applies 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:

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 that include simulation prompting a full recovery and reconstituting the information system to a known state, and that ensures that 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., organization 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 minimum-security controls determined by the impact baseline of the information system.

Office of Management and Budget

Circular 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.

Circular No. A-130, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources

Section 5(g) states that the authorization to operate an information system and the authorization of agency designated common controls granted by senior Federal officials provide an important quality control for agencies. The decision to authorize an information system to operate shall be based on a review of the authorization package and includes an assessment of compliance with applicable requirements and risk to agency operations and assets, individuals, other organizations, and the Nation. As stated above, the decision to authorize a system, or agency-defined common controls, shall be made by the appropriate authorizing official. Since the information system security plan and privacy plan establish the security and privacy controls selected for implementation, those plans are a critical part of the authorization package and shall form the basis for the authorization, supplemented by more specific information as needed.

Memorandum for Chief Information Officers – Security Authorization of Information Systems in Cloud Computing Environments -

This memo is applicable to executive departments and agencies procuring commercial and noncommercial cloud services provided by information systems that support the operations and assets of departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources. The memo also applies to all cloud service models (e.g., Infrastructure as a Service, Platform as a Service, and Software as a Service) as defined by NIST.

The memo directs each executive department or agency to use FedRAMP when conducting risk assessments, conducting security authorizations, and granting ATOs for all executive department or agency uses of cloud services.

U.S. Department of Health and Human Services

Memorandum – HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance

This memo provides HHS OpDivs with updated cloud computing security guidelines and recommendations for compliance with the FedRAMP when acquiring and/or utilizing cloud services. The memo is related to the OMB *Memorandum for Chief Information Officers – Security Authorization of Information Systems in Cloud Computing Environments.*

APPENDIX C: SECURITY DOCUMENT REVIEW TABLES

HHS Protect Security Documents

IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
1	Designation memo of information systems security officer	8/12/2020	Received 9/8/2020	Memo 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.
3	Risk assessments	8/12/2020	No	System risk assessments were not provided.
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 Personal Health Information (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	A contingency plan and test results were not provided.
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.

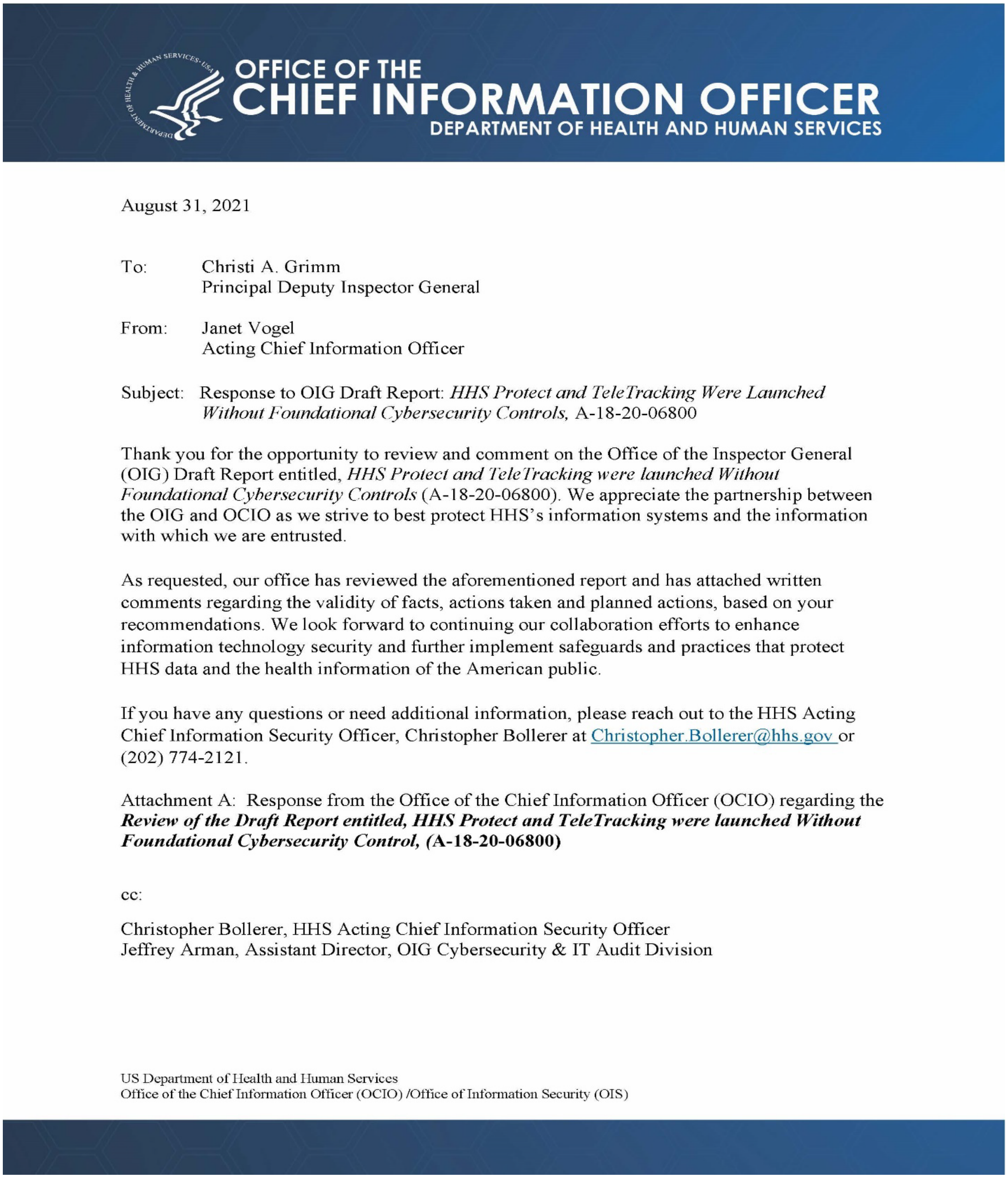
IG Control #	Information/Access/Records Requested	Date Requested	Information or Records or Access Received?	IG Analysis
8	Interconnection Security Agreement (ISA)/Memorandum of Understanding	8/12/2020	Received 1/6/2021	The ISA documents the security agreement between CDC and HHS. The document includes 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 SAR included one critical, one high, four medium, and one low severity vulnerabilities. SAR included remediation recommendations.
10	Third-party assessments	8/12/2020	No	No third-party assessments were conducted on HHS Protect.
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 authentication. 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 ATO memo without conditions was signed on 1/20/21. The HHS Protect system became operational on 4/10/2020. Conditional ATOs were issued on 4/11/20, 8/19/20, and 12/21/20, and copies were provided. Those ATOs were issued under the condition that the significant required system security assessments and documentation that had not been completed would be completed within 120 days of the memo’s issue date.

U.S. Healthcare COVID-19 Portal 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	A system security plan was not provided.
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 zero risk score and zero vulnerabilities, and an enterprise penetration test resulted in findings of one high, two moderate, and one low. These scans and/or tests demonstrated that potential risks and flaws had been assessed and addressed.
3	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 Security Management System scope.
4	International Organization for Standardization (ISO) certification	8/12/2020	Received 10/8/2020	HHS contractor 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 contractor and HHS. This document includes encryption level requirements and security-related responsibilities for the contractor and HHS.
7	Risk assessments	8/12/2020	No	System risk assessments were not provided.

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 the U.S. Healthcare COVID-19 Portal.

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)

OFFICE OF THE
CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN 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 requirements[1], 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).

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 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 documentation[2] 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;

- 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.