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On August 24, 2022, we rescinded the report because we concluded that some of the information and application of criteria in the audit regarding the U.S. Healthcare COVID-19 Portal (referred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

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.