Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

The IHS Telehealth System Was Deployed Without Some Required Cybersecurity Controls

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

September 2022
A-18-21-03100

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

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

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

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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

Report in Brief
Date: September 2022
Report No. A-18-21-03100

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

Why OIG Did This Audit

In response to the COVID-19 pandemic, health care providers increasingly deliver care using telehealth technologies. These technologies improve access to care, increase patient convenience, and increase service-delivery efficiency.

Our objective was to determine whether the Indian Health Service (IHS) implemented select cybersecurity controls to protect its telehealth system.

How OIG Did This Audit

We reviewed applicable IHS and HHS policies and procedures for telehealth technologies, interviewed staff, and reviewed system security documentation to determine whether IHS telehealth technologies was secure. We focused on determining whether IHS designed and implemented cybersecurity controls that are essential to securing IHS telehealth systems components before deployment.

The IHS Telehealth System Was Deployed Without Some Required Cybersecurity Controls

What OIG Found

Although IHS deployed a national telehealth system, which increased the availability of health care services during the pandemic, it did not complete select IT controls as required prior to deploying its telehealth system nationally. Specifically, IHS did not complete the contingency plan, risk assessment, finalized authorization to operate (ATO), and system security plan. Additionally, after deployment of the telehealth system, IHS did not remediate known vulnerabilities on some telehealth system devices in a timely manner.

Controls were not implemented because, according to IHS officials, IHS did not have a strategy for completing the requirements to implement and authorize a new information system to operate in an expedited fashion to meet an urgent, mission-critical need. IHS has since completed the controls covered by this audit, and no major incidents or breeches have been reported to HHS. However, IHS assumed an undetermined level of risk to the security of the system and data by not ensuring that all required IT controls were in place to protect the system before deployment.

What OIG Recommends and IHS Response

We recommend that the Indian Health Service develop a strategy for identifying, implementing, and testing cybersecurity controls for new information systems that are deployed in an expedited fashion to meet an urgent, mission-critical need. The strategy should define the minimum set of critical controls that must be implemented and tested before the system is deployed, noting the acceptance of risk for not implementing all required controls and stipulate that the full ATO process will be completed within a specific time period. We also recommend that the Indian Health Service ensure that adequate policies, procedures, and training are implemented to ensure that known telehealth vulnerabilities are remediated in a timely manner.

IHS concurred with our recommendations and will develop guidance for inclusion in the IHS *Indian Health Manual* for expeditiously deploying a new information system for use during emergencies when it is necessary to meet an urgent, mission-critical need. In addition, IHS will review related policies, procedures, and training to ensure that they are adequate to address all known system vulnerabilities by December 31, 2022.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182103100.asp.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

In response to the COVID-19 pandemic, health care providers and patients have increased their use of telehealth technologies to deliver care. The Indian Health Service (IHS) is dramatically increasing its reliance on telehealth to provide health care to the 2.6 million Native Americans and Alaska Natives it serves because its patients often live-in remote areas far from IHS facilities coupled with pandemic restrictions. The cybersecurity of the telehealth system that IHS uses is critical to patients' safety and health and to the privacy and integrity of their data. As the portion of IHS patients relying on telehealth increases so does the impact of a system breach. This audit focuses on IHS's cybersecurity controls for its telehealth system.

OBJECTIVE

Our objective was to determine whether IHS implemented select cybersecurity controls to protect its telehealth system.

BACKGROUND

Role of Telehealth at IHS

Native Americans and Alaska Natives often reside in locations where there is not easy access to health care. To help meet this challenge, IHS has provided health care services via telephone since the 1970s. Though telephone services remain IHS's primary means of providing telehealth, IHS has implemented other methods for providing telehealth, including videoconferencing, store-and-forward imaging,[1] streaming media, online patient portals and partnering with the National Aeronautics and Space Administration (NASA) on a co-operative that utilized space age telecommunication to provide health care.[2] In response to the COVID-19 pandemic, the IHS Chief Information Officer (CIO) authorized all IHS clinicians to use various commercial video conferencing tools to provide telehealth. The March 27, 2020, announcement stated:

> Indian Health Service clinicians may use certain additional, non-public facing audio or video communications technologies to augment all clinical activities related to providing care to patients during the COVID-19 national emergency. This applies to telehealth provided for any clinical reason, regardless of whether

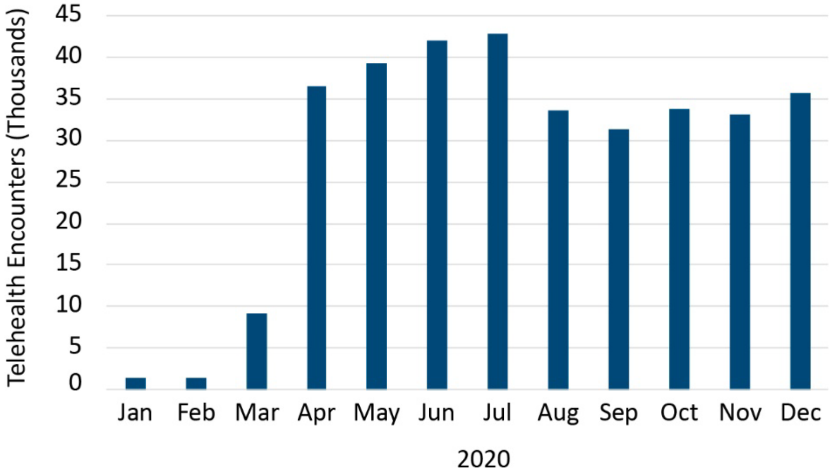
[1] Store-and-forward technology means electronic information, imaging, and communication that is transferred, recorded, or otherwise stored to be reviewed at a distant site at a later date by a health care provider or health care facility without the patient present in real time.

[2] STARPAHC (Space Technology Applied to Rural Papago Advanced Health Care) a successful co-operative project that involved the confluence of several organizations and groups, including NASA, IHS/ORD, and the Papago people to bring health care to remote parts of the Papago Reservation.

> the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19. Based on the March 17, 2020, announcement from the Office for Civil Rights (OCR) regarding Health Insurance Portability and Accountability Act (HIPAA) enforcement discretion for good faith provision of telehealth during the COVID-19 nationwide public health emergency the Indian Health Service is permitting its health care providers to communicate with patients and provide telehealth services, through the remote communications technologies, spelled out below. Even though these technologies may not fully comply with the requirements of the HIPAA rules and may potentially introduce privacy risks, IHS believes these measures are presently necessary and the benefits to patient safety and care outweigh any potential risks during this national emergency.

Immediately following the announcement, the monthly number of IHS telehealth encounters more than tripled, as shown in Figure 1.

Figure 1: 2020 IHS Telehealth Encounters Per Month



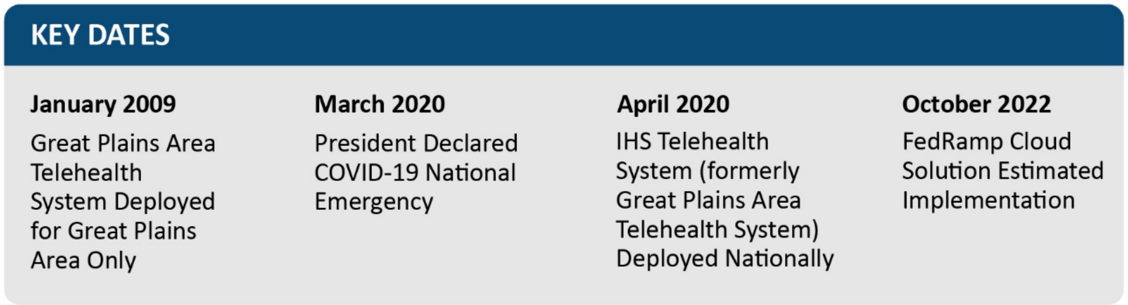
IHS Telehealth System Development

The IHS COVID-19 pandemic response included the national deployment of a telehealth system for IHS patients. Specifically, in April 2020, IHS expanded access to the Great Plains Area's telehealth system to all IHS Areas, making it the IHS telehealth system.[3] Before this expansion, the 12 IHS Areas were either not providing telehealth services or were using different telehealth systems with varying levels of functionality and reliability.

[3] The system is officially named the "Great Plains Area Cisco Meeting Server" (GCMS). Before Jan. 6, 2021, it was named the "National Telemedicine Video infrastructure and Service" (NTVIS).

In addition, IHS has an ongoing project (anticipated completion of July 2022) to upgrade part of the national IHS telehealth system to include a Federal Risk and Authorization Management Program (FedRamp)[4] cloud solution with new video conferencing hardware. This upgrade will replace system components that are no longer supported. See Figure 2 for the timeline of IHS telehealth system development.

Figure 2: IHS Telehealth System Deployment Timeline



KEY DATES

January 2009	March 2020	April 2020	October 2022
Great Plains Area Telehealth System Deployed for Great Plains Area Only	President Declared COVID-19 National Emergency	IHS Telehealth System (formerly Great Plains Area Telehealth System) Deployed Nationally	FedRamp Cloud Solution Estimated Implementation

HOW WE CONDUCTED THIS AUDIT

To accomplish our objective, we reviewed documented cybersecurity policies and procedures (listed as part of Appendix A), interviewed IHS management, and attended virtual "walk throughs" of the telehealth system and cybersecurity controls. We communicated to IHS our preliminary findings before issuing our draft report.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audit procedures to assess internal control to the extent necessary to address the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A describes our audit scope and methodology, and Appendix B contains Federal requirements and Department of Health and Human Services (HHS) guidance related to implementing cybersecurity controls.

FINDINGS

Although IHS deployed a national telehealth system, which increased the availability of health care services during the pandemic, it did not complete select IT controls as required prior to deploying its telehealth system nationally. Specifically, IHS did not complete the contingency plan, risk assessment, finalized authorization to operate (ATO), and system security plan. Additionally, after deployment of the telehealth system, IHS did not remediate known vulnerabilities on some telehealth system devices in a timely manner.

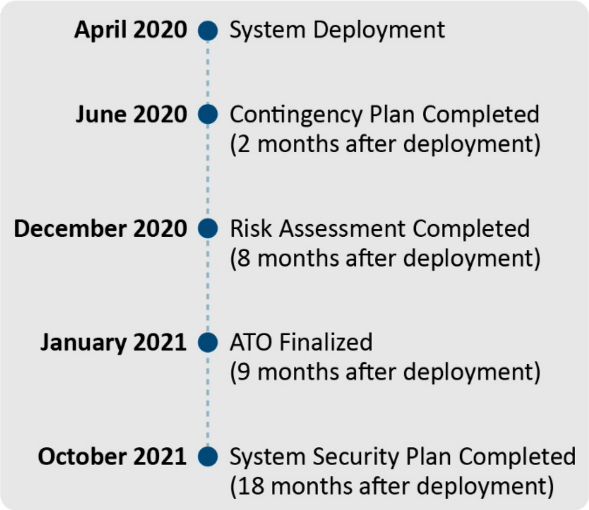
[4] FedRamp is a Governmentwide program that provides a standardized approach to assessing security, authorizing usage, and continuously monitoring cloud products and services.

Controls were not implemented because, according to IHS officials, IHS did not have a strategy for completing the requirements to implement and authorize a new information system to operate in an expedited fashion to meet an urgent, mission-critical need. IHS has since completed the controls covered by this audit, and no major incidents or breeches have been reported to HHS. However, IHS assumed an undetermined level of risk to the security of the system and data by not ensuring that all required IT controls were in place to protect the system before deployment.

IHS DID NOT IMPLEMENT REQUIRED CONTROLS BEFORE DEPLOYMENT OF THE IHS TELEHEALTH SYSTEM

IHS deployed its national telehealth system before implementing all required controls. Specifically, before the system was deployed, IHS did not complete a system security plan, contingency plan, or risk assessment and did not finalize its ATO. However, as shown in Figure 3, IHS implemented these cybersecurity controls after system deployment.

Figure 3: IHS Telehealth System Security Documentation Timeline



April 2020 ● System Deployment

June 2020 ● Contingency Plan Completed
(2 months after deployment)

December 2020 ● Risk Assessment Completed
(8 months after deployment)

January 2021 ● ATO Finalized
(9 months after deployment)

October 2021 ● System Security Plan Completed
(18 months after deployment)

IHS Did Not Complete a Contingency Plan Before System Deployment

IHS did not complete a contingency plan for the telehealth system before its deployment. Federal standards require organizations to develop contingency plans for each of their information systems. Contingency plans should contain procedures to maintain or restore information systems from a natural disaster (e.g., earthquake or hurricane) or a man-made disruption in service (e.g., ransomware or denial-of-service attack). The absence of a completed contingency plan increased the likelihood that the IHS telehealth system could not timely recover from a disruption in service, thus negatively impacting the availability of health care services to many IHS patients.

IHS completed the contingency plan 2 months after deployment of the telehealth system because, according to IHS officials, they did not have a strategy to simultaneously expedite the telehealth system deployment and complete the contingency plan prior to the telehealth system deployment.

IHS Did Not Complete a Risk Assessment Before System Deployment

IHS did not complete a risk assessment for the telehealth system before its deployment. A risk assessment is a key component of a holistic, organizationwide risk management process that includes framing, assessing, responding, and monitoring risks.[5] Without adequately assessing risks associated with the use of telehealth technology in the IHS environment, the system may have been susceptible to unacceptably high levels of unmitigated risks.

IHS initiated a risk assessment 2 months after the telehealth system was deployed and completed the assessment 6 months later. IHS officials attributed the delay of completing the risk assessment to the lack of a strategy to expedite the telehealth system deployment to combat the public health crisis while also completing required controls.

IHS Did Not Finalize Its Authorization To Operate Before System Deployment

The IHS telehealth system operated without a finalized ATO for the first 9 months of deployment. Although an interim ATO was signed when the telehealth system was deployed, it did not provide the assurance that adequate controls were in place to sufficiently mitigate risks as a finalized ATO would. In addition, the interim ATO expired 6 months before the finalized ATO was completed. The Office of Management and Budget requires Federal agencies to ensure that a management official authorizes in writing the use of the information system by confirming that its security plan as implemented adequately secures the application.[6] Without the finalized ATO, there was limited assurance that IHS management had sufficiently secured the telehealth system, which could put personally identifiable health information at increased risk of unauthorized disclosure or manipulation.

IHS management did not finalize the ATO until 9 months after deployment because IHS lacked a strategy to expedite system deployment to respond to the public health emergency while also finalizing the ATO requirements.

IHS Did Not Complete a System Security Plan Before System Deployment

IHS did not complete a system security plan for the telehealth system before its deployment. Federal standards require organizations to develop for each of its information systems a

[5] National Institute of Standards and Technology Special Publication (NIST SP) 800-30, *Guide for Conducting Risk Assessments.*

[6] Circular No. A-130, *Appendix III: Security of Federal Automated Information Resources*, section A(3)(b)(4).

security plan that describes cybersecurity threats and the controls in place to meet security and privacy requirements before system deployment.[7] Without the security plan, IHS had limited assurance that controls were implemented to meet security requirements and mitigate identified threats. Additionally, the security plan is to be completed prior to completing the finalized ATO, so that the authorizing official can use it in determining whether controls had been identified, in place, and operating effectively.

IHS completed the system security plan 18 months after the telehealth system was deployed. Completion of the plan was delayed because IHS lacked a strategy to focus on expediting the telehealth system deployment in response to the public health emergency while also completing the security plan.

IHS DID NOT REMEDIATE KNOWN VULNERABILITIES ON TELEHEALTH DEVICES IN A TIMELY MANNER

IHS performed continuous monitoring of the IHS telehealth system devices identified in its system security plan.[8] However, we determined that eight of these devices had "known vulnerabilities" that were not remediated in a timely manner.[9] Specifically, we found that telehealth devices contained these vulnerabilities for up to 10 months before being remediated. Federal organizations are required to identify, report, and remediate vulnerabilities in a timely manner.[10] Without timely remediation of vulnerabilities, the system and the data it contains are at an increased risk for unauthorized disclosure, alteration, and destruction.

We shared this information with IHS officials, and verified they remediated all the "known vulnerabilities" that we had identified. IHS officials were unable to provide a reason the vulnerabilities were not remediated in a timely manner because those responsible were no longer at the agency.

RECOMMENDATIONS

We recommend the following:

- The Indian Health Service should develop a strategy for expeditiously deploying a new information system when it is necessary to meet an urgent, mission-critical

[7] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

[8] These devices consisted of Cisco Meeting servers, video communication and recording servers, file servers, virtual servers, and a load balancer.

[9] A "known vulnerability" is a publicly disclosed computer security flaw that has been assigned a Common Vulnerability Exposure (CVE) identification number.

[10] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

need. The strategy should define the minimum set of controls out of the total number of required controls that should be addressed and, if applicable tested, before the new system is authorized to operate until it is feasible to address all required controls. The authorization to operate should include an acceptance of risk for not implementing all required controls, specify a date by which the remaining required controls will be implemented and tested, and be replaced with a new authorization to operate once all the required controls have been addressed.

- The Indian Health Service should ensure adequate policies, procedures and training are implemented to ensure that known vulnerabilities that may impact the telehealth technologies are remediated in a timely manner.

IHS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments, IHS concurred with our recommendations and said that it will develop guidance for inclusion in the IHS *Indian Health Manual* (IHM) for expeditiously deploying a new information system for use during emergencies when it is necessary to meet an urgent, mission-critical need. In addition, IHS will review related policies, procedures, and trainings to ensure they are adequate to address all known system vulnerabilities by December 31, 2022.

IHS's comments are included in their entirety as Appendix C.

We are encouraged that IHS has made such substantial and commendable progress to improve system development and security. This progress includes defining the minimum set of controls needed before system authorization in the IHS IHM Chapter and the strengthening of controls to ensure that all known system vulnerabilities are adequately addressed.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We analyzed select IHS telehealth cybersecurity controls to determine whether they complied with NIST standards and HHS and IHS policies. We used NIST controls for telehealth environments as a baseline to determine whether required controls were completed.

We conducted our audit work from January 2021 thru June 2022.

METHODOLOGY

To accomplish our objective, we requested and reviewed IHS's documentation related to ensuring the confidentiality, integrity, and availability of IHS telehealth technologies. We also interviewed IHS personnel to gain an understanding of implemented controlsI

.

We assessed the following IHS Telehealth IT controls to determine whether IHS complied with the Federal requirements for:

- ATO – An official management decision to authorize operation of an IT system and to explicitly accept the risk to organizational operations based on the implementation of an agreed-upon set of controls.

- Contingency Plan – A 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).

- Risk Assessment – The process of identifying and documenting the risks to an information system; it is part of risk management and incorporates threat and vulnerability analyses.

- Privacy Impact Assessment – An analysis and documentation of how information is handled 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.

- System Security Plan (SSP) – A formal document that provides an overview of the security requirements for an IT system and describes the controls in place or planned for meeting those requirements and for mitigating identified threats.

- Vulnerability Assessment – A systematic examination of an IT system or product to determine the adequacy of security measures.

We designed our audit to determine whether these IT controls were implemented to secure IHS telehealth technologies in accordance with Federal requirements; our audit was not an assessment of organizational internal controls.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audit procedures to assess internal control to the extent necessary to address the 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 HHS GUIDANCE

FEDERAL REQUIREMENTS

Federal Information Security Modernization Act of 2014

Section 3554 states that:

> 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).

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.

National Institute of Standards and Technology Standards and Special Publications

NIST Federal Information Processing Standards (FIPS) Publication 199: *Standards for Security Categorization of Federal Information and Information Systems*, established a standard for categorizing Federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability:

> 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.

NIST FIPS 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*.

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 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

> For an information system, authorizing officials issue an authorization to operate or authorization to use for the system, accepting the security and privacy risks to the organization’s operations and assets, individuals, other organizations, and the Nation. (See the publication’s Appendix F, page 13).

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:

- contingency planning,
- risk assessment,
- security assessment and authorization.

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.

HHS AND IHS GUIDANCE

HHS Information Systems Security and Privacy Policy (IS2P)

IS2P is the HHS policy that establishes baseline IT security and privacy requirements for the HHS operating divisions' IT security programs and information systems. (Operating divisions may complement IS2P by developing their own policies and procedures.)

Enterprise Performance Life Cycle Framework Security Deliverables Documents

The HHS Enterprise Performance Life Cycle (EPLC) framework applies to all HHS IT investments and projects, including, but not limited to, new projects; major enhancements to existing projects; projects associated with steady-state investments;[11] high-priority, fast-track IT projects; and new Commercial Off-the-Shelf (COTS) product acquisitions.

The EPLC framework organizes the activities, deliverables, and governance reviews of an IT project into 10 life-cycle phases. The EPLC framework provides a project management methodology that guides the activities of project managers, business owners, critical partners, IT governance organizations, and other stakeholders throughout the life cycle of the project to ensure an enterprise perspective is maintained during planning, execution, and governance processes. Although one of the objectives of the EPLC framework is to standardize IT project management within HHS based on best practices, the framework also allows tailoring to accommodate the specific circumstances (e.g., size, duration, complexity, and acquisition strategy) of each project.

Indian Health Manual (IHM), Chapter 12 – Information Technology Security

This chapter requires each IHS automated information system to have a level of security commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system.

[11] At the steady-state, an investment is equal to depreciation, which means that all of the investment is being used to repair and replace the existing capital stock.

APPENDIX C: IHS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Indian Health Service
Rockville, MD 20857

DATE: August 12, 2022

TO: Inspector General

FROM: Acting Director

SUBJECT: IHS Response to Draft OIG Report: *IHS Telehealth System Was Deployed Without Some Required Cybersecurity Controls* (A-18-21-03100), dated June 29, 2022

We appreciate the opportunity to provide our official comments on the Draft Office of Inspector General (OIG) Report entitled, *IHS Telehealth System Was Deployed Without Some Required Cybersecurity Controls* (A-18-21-03100), dated June 29, 2022. The Indian Health Service (IHS) concurs with the two OIG recommendations discussed below.

Recommendation Number 1: IHS concurs with the recommendation.

The Indian Health Service should develop a strategy for expeditiously deploying a new information system when it is necessary to meet an urgent, mission-critical need. The strategy should define the minimum set of controls out of the total number of required controls that should be addressed and, if applicable tested, before the new system is authorized to operate until it is feasible to address all required controls. The authorization to operate should include an acceptance of risk for not implementing all required controls, specify a date by which the remaining required controls will be implemented and tested, and be replaced with a new authorization to operate once all the required controls have been addressed.

Planned and completed actions:

The IHS will develop guidance for inclusion in the IHS Indian Health Manual (IHM) for expeditiously deploying a new information system for use during emergencies when it is necessary to meet an urgent, mission-critical need by March 31, 2023.

The IHS IHM Chapter will define the minimum set of controls out of the total number of required controls addressed by the System Owner and, if applicable, tested before the new system is authorized to operate until it is feasible to address all required controls.

The IHS guidance will ensure that all of the required controls (i.e. Contingency Plan, ISA, SSP, ATO, FedRAMP approval, etc.) are addressed/implemented and tested prior to the new system being authorized to operate and be deployed.

Recommendation Number 2: IHS concurs with the recommendation

The Indian Health Service should ensure adequate policies, procedures and training are implemented to ensure that known vulnerabilities that may impact the telehealth technologies are remediated in a timely manner.

Planned and completed actions:

By December 31, 2022, the IHS will review related policies, procedures, and trainings to ensure they are adequate to address all known system vulnerabilities. New solutions such as Crowdstrike, Technopedia, and MS CASB are under development to help identify vulnerabilities. Fully implementing policies and procedures to address vulnerabilities in the IHS telehealth solution is a top priority.

Thank you for the opportunity to review and comment on this draft report. Please refer any follow up questions you have regarding our comments to Ms. Athena Elliott, IHS Chief Compliance Officer by email at athena.elliott@ihs.gov. Questions about the program may be directed to Mr. Mitchell Thornbrugh, Chief Information Officer by email at mitchell.thornbrugh@ihs.gov.

Elizabeth A. Fowler -S
Digitally signed by Elizabeth A. Fowler - S
Date: 2022.08.12 03:04:55 -04'00'

Elizabeth A. Fowler