United States Government Accountability Office

Report to Congressional Requesters

December 2021

CYBERSECURITY

NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program

Accessible Version

GAO Highlight

Highlights of GAO-22-104467, a report to congressional requesters

December 2021

CYBERSECURITY

NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program

Why GAO Did This Study

NIH responsibilities include conducting research on the prevention of infectious diseases such as COVID-19, administering over $30 billion annually in medical research grants, and supporting research on pathogens, including those that have the potential to pose a severe threat to public health and safety. In carrying out its mission, NIH relies extensively on information technology systems to receive, process, and maintain sensitive data. Accordingly, effective information security controls are essential to ensure the confidentiality, integrity, and availability of the agency's systems.

GAO was asked to examine cybersecurity at NIH. In June 2021, GAO issued a limited official use only report on the extent to which NIH had effectively implemented system controls and an information security program to protect the confidentiality, integrity, and availability of its information on selected information systems.

This current report is a public version of the June 2021 report based on GAO's review of the agency's information security program and 11 selected systems. In addition, for this public report, GAO determined the extent to which NIH has taken corrective actions to address the previously identified security program and system control deficiencies and related recommendations for improvement. GAO reviewed supporting documents regarding NIH's actions on the previously identified recommendations.

View GAO-22-104467. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

As GAO reported in June 2021, the U.S. National Institutes of Health (NIH) implemented information security controls—both for its security program and selected systems—intended to safeguard the confidentiality, integrity, and availability of its information systems and information. However, GAO identified numerous control and program deficiencies in the core security functions related to identifying risk, protecting systems from threats and vulnerabilities, detecting and responding to cyber security events, and recovering system operations (see table). GAO made 219 recommendations—66 on the security program and 153 related to system controls—to address these deficiencies.

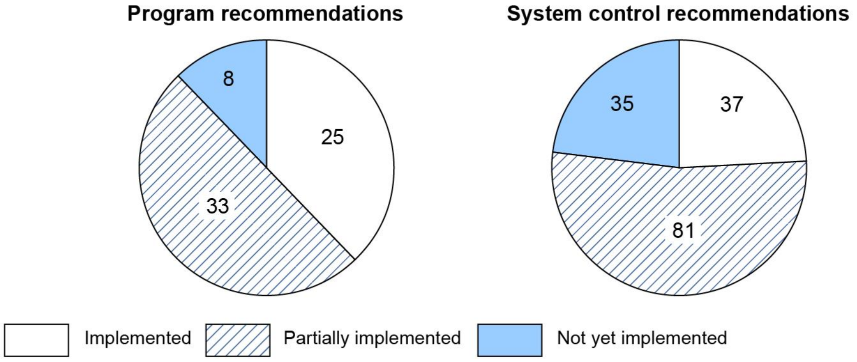
Number of GAO-Identified Information Security Program and Control Deficiencies at the U.S. National Institutes of Health and Associated Recommendations by Core Security Function as of June 2021

Core security function	Number of information security program deficiencies	Number of information security program recommendations	Number of selected system control deficiencies	Number of selected system control deficiency recommendations
Identify	12	26	0	0
Protect	4	6	78	141
Detect	5	11	5	11
Respond	7	16	1	1
Recover	4	7	0	0
Total	32	66	84	153

Source: GAO. | GAO-22-104467

As of June 2021, NIH had made progress in resolving the deficiencies by implementing 25 (about 38 percent) of the 66 information security program recommendations, and 37 (about 24 percent) of the 153 recommendations to address control deficiencies for selected systems. The figure shows the status of NIH's efforts to implement the 219 recommendations.

Status of GAO Recommendations to the U.S. National Institutes of Health as of June 2021



Source: GAO analysis of National Institutes of Health data. | GAO-22-104467

Accessible Data Table for Highlight Figure

	Implemented	Partially implemented	Not yet implemented
Program Recommendations	25	33	8
System Control Recommendations	37	81	35

Until NIH fully implements these recommendations and resolves the associated deficiencies, its information systems and information will remain at increased risk of misuse, improper disclosure or modification, and destruction.

Contents

GAO Highlight 2

Why GAO Did This Study 2

What GAO Found 2

Letter 1

Background 8

Security Program and System Control Deficiencies Place Selected NIH Information Systems at Risk 12

NIH Has Fully Implemented about 28 Percent of Our Recommendations and Partially Implemented about 52 Percent 61

Agency Comments and Our Evaluation 65

Appendix I: Objectives, Scope, and Methodology 67

Appendix II: National Institute of Standards and Technology's Cybersecurity Framework 76

Appendix III: Comments from the Department of Health and Human Services 81

Agency Comment Letter 87

Appendix IV: GAO Contact and Staff Acknowledgments 94

Tables

Table 1: GAO Assessment of Security Controls in Selected U.S. National Institutes of Health (NIH) Entities' System Security Plans,* as of September 2019 24

Table 2: Extent to Which the U.S. National Institutes of Health Developed, Documented, and Reviewed Policies and Procedures as Outlined by the NIST SP 800-53 Security Control Areas* 29

Table 3: GAO Assessment of U.S. National Institutes of Health (NIH) Control Assessments for 11 Selected Systems as of July 2019 46

Table 4: Plans of Action and Milestones Older Than 2 Years as of December 2019, by Assigned Risk, at One Selected Entity of the U.S. National Institutes of Health (NIH) 58

Table 5: Number of Identified Control and Information Security Program Deficiencies at U.S. National Institutes of Health and Associated Recommendations by Core Security Function as of June 2021 63

Table 6: Status of Efforts by U. S. National Institutes of Health (NIH) to Implement GAO's Recommendations for Selected System Control Deficiencies by Core Security Function, as of June 2021 63
Table 7: Status of Efforts by U.S. National Institutes of Health (NIH) to Implement GAO's Recommendations for Improving its Information Security Program by Core Security Function, as of June 2021 64
Table 8: National Institute of Standards and Technology Cybersecurity Framework 76

Figures

Figure 1: GAO Assessment of U.S. National Institutes of Health (NIH) Actions to Address Five Key Risk Assessment Steps for 11 Selected Information Systems in Four Selected Entities, as of December 2019 19
Figure 2: GAO Assessment of Required Elements of Selected U.S. National Institutes of Health (NIH) Entities' System Security Plans, as of September 2019 23
Figure 3: Process Used by NIH, HHS, and DHS to Coordinate on Information Security Incidents 51
Figure 4: GAO Assessment of U.S. National Institutes of Health (NIH) Selected Entities' Implementation of Required Elements of Plans of Action and Milestones for Selected Systems 55
Figure 5: GAO Assessment of U.S. National Institutes of Health (NIH) Selected Entities' Implementation of Contingency Planning Requirements for 11 Selected Information Systems 60

Abbreviations

BSL	biosafety level
CIO	chief information officer
CISO	chief information security officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GSS	general support system
HHS	Department of Health and Human Services
ISAO	Information Security and Awareness Office
ISCM	information security continuous monitoring
ISSO	information systems security officer
LOUO	limited official use only
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OD	Office of the Director
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of action and milestones
SIEM	security information and event management
SP	Special Publication
TMIR	Threat Mitigation and Incident Response

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

December 7, 2021

The Honorable Frank Pallone, Jr.
Chairman
The Honorable Cathy McMorris Rodgers
Republican Leader
Committee on Energy and Commerce
House of Representatives

The Honorable Morgan Griffith
Republican Leader
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Fred Upton
House of Representatives

The U.S. National Institutes of Health (NIH)—an operating division of the Department of Health and Human Services (HHS)—serves as the national focal point for publicly funded biomedical research. The agency's mission is to discover and apply medical knowledge that enhances health, lengthens life, and reduces illness and disability. This includes conducting research on the prevention of infectious diseases, such as the Coronavirus Disease 2019 (COVID-19). NIH advances its mission by conducting research in its own laboratories; supporting the research of non-federal scientists in universities, medical schools, hospitals, and research institutions throughout the U.S. and abroad; helping in the training of research investigators; and communicating medical and health sciences information.

NIH uses information technology (IT), such as high-performance computing, to aid in accomplishing its mission. However, recent cyberattacks demonstrate the damage that increasingly sophisticated cyber threats can cause to federal IT systems. The seriousness of this threat was reinforced by the December 2020 discovery of the SolarWinds cyberattack that had a widespread impact on government agencies.

Since 1997, we have designated the security of information of federal systems (i.e., information security) to be a government-wide high-risk area. In 2003, we expanded the area to include securing the computerized systems supporting the nation’s critical infrastructure and, in 2015, we included protecting the privacy of personally identifiable information.[1]

Given the critical role that NIH performs, and concerns over the security of federal information systems, you requested that we examine the security controls over key NIH information systems. Our specific objective was to determine the extent to which NIH has effectively implemented information security controls to protect the confidentiality, integrity, and availability of its information on selected information systems.

In June 2021, we issued a report that addressed the extent to which NIH had effectively implemented an information security program and controls to protect the confidentiality, integrity, and availability of its information on selected information systems.[2] In the report, we made 153 recommendations to NIH to resolve system security control deficiencies (referred to as system controls in this report) in the information systems we reviewed and 66 additional recommendations to improve the agency’s information security program. We designated that report as “limited official use only” (LOUO) and did not release it to the general public because of the sensitive information it contained.

This subsequent report publishes the findings discussed in our June 2021 report, but we have removed all references to the sensitive information. Specifically, we deleted the names of the information systems and computer networks that we examined, disassociated identified control deficiencies from named systems, deleted certain details about information security controls and control deficiencies, deleted conclusions and recommendations, and omitted an appendix that was contained in the LOUO report. The appendix contained sensitive details about the system control deficiencies in NIH’s information systems that we reviewed, and the 153 recommendations we made to mitigate those deficiencies. The body of the report contained 66 recommendations we made for NIH to improve its security program. We also provided a draft of this report to NIH officials to review and comment on the sensitivity of the

[1] For our latest high-risk report, see GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar 2, 2021).

[2] GAO, *Cybersecurity: NIH Needs to Address Program and Control Deficiencies That Put Mission and Public Health Data at Risk*, GAO-21-333SU (Washington, D.C.: June 30, 2021).

information contained herein and to affirm that the report can be made available to the public without jeopardizing the security of NIH's systems.

In addition, this report addresses a second objective that was not included in the June 2021 report. Specifically, this objective was to determine the extent to which NIH has taken corrective actions to address the previously identified security program and system control deficiencies and related recommendations for improvement that we identified in the earlier report.

As noted in our LOUO report, to accomplish our first objective, we selected a risk-based, non-generalizable sample from the 123 reported information systems that NIH uses for biosafety labs, biomedical research, high performance computing, facilities maintenance, and administration. To do so, we focused on systems that: (1) collect, process, and maintain private or potentially sensitive proprietary business, personal medical health records, or personally identifiable information; (2) are essential to NIH's mission; (3) provide applications and controls for Biosafety Levels (BSL) 3 and 4 labs[3] that contain select agents,[4] which, if compromised, could pose a severe threat to public safety; and/or (4) share some common infrastructure.

We also took into consideration entities from among the agency's 28 institutes, centers, and the Office of the Director.[5] Our selection focused on entities that provide information technology and security for NIH and that are essential to the agency's mission.

[3] Biosafety levels (BSL) are used to identify the protective measures needed in a laboratory setting to protect workers, the environment, and the public. Research on agents not known to consistently cause disease in healthy adults is conducted in BSL-1 labs. Research on moderate-risk agents that pose a danger if accidentally inhaled, swallowed, or exposed to the skin is conducted in BSL-2 labs. Research on agents that can be transmitted through the air and cause potentially lethal infection is conducted in BSL-3 labs. Research on agents that pose a high risk of life-threatening disease for which no vaccine or therapy is available is conducted in BSL-4 labs.

[4] Select agents are biological agents and toxins that have the potential to pose a severe threat to public health and safety, to animal and plant health, or to animal or plant products.

[5] In this report, we use the term "entities" to represent NIH's institutes, centers, and office.

Based on applying these criteria to systems and entities, we selected 11 mission-essential systems within four entities.[6] Of these systems, the agency had categorized five as high-impact systems, five as moderate-impact systems, and one as a low-impact system.[7] The agency also considered one system to be a high-value asset that is of particular interest to potential adversaries.[8]

To evaluate NIH's information security controls—both for its information security program and selected systems—we based our assessment of controls on requirements of the Federal Information Security Modernization Act of 2014 (FISMA),[9] which establishes key elements for an effective agency-wide information security program; National Institute of Standards and Technology (NIST) guidelines and standards;[10] HHS and NIH policies, procedures, and standards; and standards and guidelines from relevant security organizations, such as the National

[6] We are not naming the four selected entities in this report due to the sensitive nature of the information.

[7] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: February 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

[8] High-value assets refer to those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical federal operations, or house unique collections of data (by size or content), making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. government.

[9] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[10] For example, see National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006), and National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

Security Agency, the Center for Internet Security,[11] and the Interagency Security Committee.[12] In addition, to evaluate NIH's controls over its information systems, we used our *Federal Information System Controls Audit Manual,* which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.[13]

For reporting purposes, we categorized the security controls that we assessed into the five core security functions described in the NIST cybersecurity framework.[14] These five core security functions are identify, protect, detect, respond, and recover, which are discussed as follows:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[15]
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

[11] The Center for Internet Security is a nonprofit entity that uses a global information technology community to safeguard private and public organizations against cyber threats. The Center also provides tools to assess implementation of industry best practices for information system security controls, such as firewall rules and policy settings. We used a Center for Internet Security tool to assess NIH's information systems.

[12] The Interagency Security Committee, an interagency organization chaired by the Department of Homeland Security, was established by Executive Order No. 12977, 60 Fed. Reg. 54411 (October 1995), to enhance the quality and effectiveness of security and the protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities. Executive Order No. 12977 was later amended by Executive Order No. 13286, 68 Fed. Reg. 10619 (March 2003). The organization is comprised of senior level executives from federal agencies and departments.

[13] GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009).

[14] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

[15] According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

For the *identify* core security function, we examined the agency's information system inventory as well as policies, procedures, and practices for consistency with guidance. In addition, for selected systems, we analyzed impact categorizations, risk assessments, and system authorization documentation to determine whether NIH identified threats, vulnerabilities, and impact from the loss of confidentiality, integrity, or availability.[16] Further, we examined authorization process documentation for consistency with guidance. We also reviewed the 11 selected systems' security plans to determine if those plans had been developed, documented, and updated according to federal guidance.

For the *protect* core security function, we reviewed the technical controls associated with user access, authorization, network integrity, physical access, and cryptography for the 11 selected systems. In addition, we analyzed the four selected entities' basic security awareness and cybersecurity role-based training records to determine if employees and contractors had received security awareness training in accordance with federal requirements, and whether personnel who had significant security responsibilities had received training commensurate with those responsibilities.

For the *detect* core security function, we reviewed the technical controls associated with logging and monitoring for the 11 selected systems. We also analyzed NIH's security control assessments for these selected systems to determine whether the agency had sufficiently and periodically tested controls for the systems. In addition, we reviewed NIH's implementation of its continuous monitoring strategy to determine whether the agency had implemented controls to, among other things, detect threats and manage vulnerabilities.

For the *respond* core security function, we reviewed the technical controls associated with the agency's forensic analysis practices. We also reviewed NIH's implementation of incident response plans and remedial

[16] A security authorization is the decision made by a senior official to put an information system into operation, based on a defined system boundary, and to explicitly accept the risk to the organization.

actions to determine whether the plans and actions were consistent with guidance.

For the *recover* core security function, we examined the contingency plans for the selected systems to determine whether the agency had developed, tested, and annually reviewed plans to ensure that critical operations could continue without interruption.

We supplemented our analyses with interviews of NIH personnel and observations of physical and environmental security controls. We conducted our reviews at agency facilities located in Bethesda and Frederick, Maryland; Hamilton, Montana; and Ashburn and Sterling, Virginia.

To determine the reliability of NIH's computer-processed data for information system inventories, user access, and training, we reviewed related documents, interviewed knowledgeable agency officials, and reviewed controls over that data. Through these methods, we concluded that the data were sufficiently reliable for the purposes of our work, except for deficiencies noted in this report.

To accomplish our second objective—to determine the extent of NIH's actions to address each recommendation that the agency indicated it had implemented as of June 4, 2021—we examined supporting documents to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve the underlying control deficiency. Based on this assessment, we categorized the status of each recommendation as being implemented, partially implemented, or not implemented. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from January 2019 to December 2021 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In order to accomplish its mission, NIH has approximately 48,000 personnel across the U.S.[17] For fiscal year 2019, the agency's total appropriation was $39 billion, of which it reported spending $1.15 billion on IT and $114.9 million (or about 10 percent of all IT spending) on information security.

In addition to its appropriations, NIH received $15.9 million in information security funding from HHS and the Department of Homeland Security (DHS) in fiscal year 2019.[18] For fiscal year 2020, NIH's total appropriation was $41.8 billion, of which it reported spending $1.23 billion on IT and $145.9 million (or about 12 percent of all IT spending) on information security.

NIH Uses a Federated Model of Management

NIH is made up of 28 entities: the Office of the Director (OD), 21 institutes, and six centers. OD operates as NIH's central managing office. In this capacity, it has responsibility for setting policy, and for planning, managing, and coordinating overall NIH programs and activities, including information technology and security. In addition, each institute has a specific research agenda that often focuses on particular diseases or body systems. The six centers vary in function, to include research, program support, patient care, and other NIH-wide services.

NIH has established key offices and officials with responsibilities for information security. Specifically, the agency's Office of the Chief Information Officer (OCIO) resides within OD and has responsibility for leading and communicating the strategic direction and management of significant information security/IT policies and procedures. The NIH chief information officer (CIO) reports quarterly to the HHS CIO on the overall effectiveness of NIH's information security and privacy program across all entities, including any remedial actions. HHS provides the agency with

[17] The 48,000 personnel include approximately 19,500 federal employees; 19,700 contractor staff; 4,700 fellows; and 3,600 volunteers, tenants, and guests.

[18] NIH received funding from HHS and DHS to purchase and implement information security tools.

guidance, support for security tools, and information on cybersecurity threats.[19]

In addition, the CIO designates a chief information security officer (CISO), who oversees entity compliance with the agency's information security and privacy requirements. NIH also created the Information Security Awareness Office (ISAO), which manages and operates the agency's information security program across all entities. The CISO and ISAO, among other things, are responsible for providing information security awareness training to employees, responding to information security incidents, scanning for vulnerabilities, and assisting entities with their information security. Further, in most cases, the CISO approves entities' authorizations to operate for their major applications and general support systems, and accepts the risks introduced by those systems.

Each of the NIH entities is responsible for its business operations and mission needs, including information security operations. Each entity designates its own CIO, who reports to and coordinates with the NIH CIO. Each CIO is responsible for establishing a computer security incident response team, ensuring that information security policies and processes are consistent with NIH and HHS security requirements, and appointing an entity CISO and/or information systems security officer (ISSO). The entity CISO or ISSO is responsible for managing the information security program within the entity, which includes keeping information systems up to date with vendor-issued security patches; appropriately managing user access privileges; providing role-based security training to users who have significant security responsibilities; and identifying and reporting security incidents to the NIH CISO, among other duties.

NIH relies extensively on information systems for biomedical research, high performance computing, facilities maintenance, intramural biosafety labs, and administration. The agency's information systems also support research and training conducted at approximately 2,500 universities and medical centers.

[19] We previously issued a report examining the information sharing between the department and its operating divisions, such as NIH. See GAO, *Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, GAO-21-403 (Washington, D.C.: June 28, 2021).

Federal Law and Guidance Establish Security Requirements to Protect Federal Information and Systems

The *Federal Information Security Modernization Act of 2014* (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over federal operations and assets. FISMA assigns responsibility to each agency head for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The law also delegates to the agency CIO (or comparable official) the authority to ensure compliance with FISMA requirements. The CIO is responsible for designating a senior agency information security officer whose primary duty is information security.

The law also requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency. Such a program includes assessing risks; developing and implementing policies and procedures to cost-effectively reduce risks; developing and implementing plans for providing adequate information security for networks, facilities, and systems; providing security awareness training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; developing and implementing procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations. In addition, FISMA requires agencies to comply with NIST standards and the Office of Management and Budget (OMB) requires agencies to comply with NIST guidelines.

NIST Federal Information Processing Standards (FIPS) Publication 199 requires agencies to categorize systems 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. NIST FIPS 200 requires agencies to meet minimum security requirements by selecting the appropriate security controls,[20] as described in NIST Special Publication (SP) 800-53.[21]

SP 800-53 provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets.[22] The publication provides baseline security controls for low-, moderate-, and high-impact systems, and agencies have the ability to tailor or supplement their security requirements and policies based on agency mission, business requirements, and operating environment.

Further, in May 2017, the President issued an executive order[23] requiring agencies to immediately begin using NIST's cybersecurity framework for managing their cybersecurity risks.[24] The framework, which provides guidance for cybersecurity activities, is based on five core security functions:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

[20] National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006).

[21] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

[22] Security control topics, referred to as families of security controls, covered by Special Publication 800-53 include access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

[23] The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

[24] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Gaithersburg, MD: Apr. 16, 2018). The framework was developed in response to an executive order issued by a prior administration (The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013)). It was originally intended for use in protection of critical infrastructure. NIST initially issued guidance in February 2014 and has since revised the framework.

- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

According to NIST, these five functions occur concurrently and continuously, and provide a strategic view of the life cycle of an organization's management of cybersecurity risk. Within the five functions are cybersecurity activities organized into 23 categories and 108 subcategories.[25] Appendix II provides a description of the framework categories and subcategories of controls.

Security Program and System Control Deficiencies Place Selected NIH Information Systems at Risk

NIH had implemented numerous security controls over the 11 systems we reviewed. These controls included, among other things, taking steps to develop security plans, ensure that the majority of personnel had basic security awareness training, and develop remedial action plans.

However, the agency had not always effectively implemented other controls—both within its information security program and for the selected systems—to protect the confidentiality, integrity, and availability of these systems and the information maintained on them. Deficiencies existed in controls intended to identify risk, protect systems from threats and

[25] For example, "risk assessment" is one of five categories that comprise the "identify" function. The risk assessment category is divided into six subcategories that involve activities such as identifying and documenting internal and external threats; identifying potential business impacts and likelihoods; and determining risk based on threats, vulnerabilities, likelihoods, and impacts. Each subcategory activity cross-references information system controls from various information security publications, including NIST SP 800-53.

vulnerabilities, detect cybersecurity events, respond to these events, and recover system operations.

These deficiencies increased the risk that sensitive research and health-related information could be disclosed or disrupted.

NIH Addressed System Identification, Risk Assessment, Planning, and Accountability, but Several Shortcomings Existed

Controls associated with the *identify* core security function are intended to help an agency develop an understanding of its resources and related cybersecurity risks to its systems, assets, data, and capabilities.[26] These controls include developing and reporting an inventory of major information systems, categorizing systems based on the potential impact of disruption or misuse, identifying and assessing cybersecurity risk, authorizing systems to operate, and establishing information security policies, procedures, and plans.

Although NIH took steps to implement these controls, the agency did not

- develop and report a complete inventory of all major information systems;
- categorize systems in a manner consistent with guidance;
- fully develop a risk management strategy and assess risks for reviewed systems;
- fully develop and document system security plans;
- consistently authorize systems based on defined system boundaries; and
- fully document and review policies and procedures.

NIH Took Steps to Develop and Report an Inventory of Major Information Systems, but the Inventory Was Incomplete

FISMA requires that each agency develop and maintain an inventory of major information systems operated by the agency or entities under its

[26] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

control.[27] Consistent with FISMA, NIST defines an information system as a discrete set of information resources organized for, among other things, the collection, maintenance, or disposition of information. A complete and accurate inventory of major information systems is a key element of managing the agency's information technology resources, including the security of those resources. The inventory is an important tool in tracking agency systems for oversight, as well as purposes such as implementation and assessment of security controls.

OMB, consistent with FISMA, also requires agencies to develop and maintain an inventory of information systems. OMB and DHS require agencies to submit an inventory of information systems, as well as the associated impact levels, as part of quarterly and annual FISMA reports.[28] HHS and NIH policies align with OMB requirements, and provide specific guidance on inventory development and reporting. In addition, NIH assigns responsibility for managing and reporting the system inventory to both the CIO and its entities.[29]

NIH took steps to develop, maintain, and report an inventory of major information systems; however, the agency did not completely and accurately report 20 systems in its FISMA inventory report provided to OMB and DHS. Specifically, NIH submitted a May 2019 FISMA inventory that reported a total of 55 major information systems, of which seven were high impact. However, as of May 2019, our review identified 75 total major information systems, of which 14 were high impact. Specifically, the following systems were not reported:

- NIH did not identify and report a spreadsheet used by an entity for tracking and maintenance of specialized critical data as a high-impact system. The entity had decided to process information outside the

[27] The inventory requirement of 44 U.S.C. § 3505 was added by the *Paperwork Reduction Act of 1995* and was subsequently amended by FISMA 2002. Title 44 of the U.S. Code specifically defines an information system as a discrete set of information resources organized for, among other things, the collection, maintenance, or disposition of information. 44 U.S.C. § 3502.

[28] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[29] Department of Health and Human Services, *HHS System Inventory Management Standard,* version 2.0 (Washington, D.C.: Dec. 27, 2018). NIH policy requires components to develop and maintain an inventory of their information systems and provide this information to the Information Security and Awareness Office within the Office of the Chief Information Officer. National Institutes of Health, *NIH Information Security Handbook*, version 5 (Bethesda, MD: Jan. 9, 2019).

system intended to protect the data. As such, the activity constituted use of a discrete set of resources—i.e., a workstation, spreadsheet application, and data that were not part of a defined system.

- The agency did not report 13 systems because, according to OCIO officials, the agency considered them to be components of five general support systems (GSS). However, documentation such as system security plans did not corroborate these designations. For example, OCIO officials reported a high-impact major information system as being a component of an entity's GSS. However, the system's documentation stated that it was a major information system. In addition, the entity's GSS system security plan said the GSS only consisted of network devices and did not include the high-impact system as a component.
- The agency did not report six systems, which OCIO officials said should have been included in the FISMA inventory report. The officials stated that they included or planned to include the systems in subsequent reports.[30]

OCIO officials provided various reasons for the inventory deficiencies. Specifically:

- Regarding the unidentified system used to collect, track, and maintain critical data, OCIO officials and the entity's CIO said that because the agency maintained the data on a spreadsheet, they had decided not to identify it as a system. In addition, agency officials said that they would not and could not control the usage of such spreadsheets within their organization. However, NIH's decision was inconsistent with NIST and agency guidance, which defines an information system as a discrete set of information resources organized for, among other things, the collection, maintenance, or disposition of information.
- Regarding the 13 systems that the agency identified as components of other systems, officials cited flexibility in NIST guidance for determining what constitutes an information system. While NIST allows for this flexibility, the agency's reporting and inventory of what constituted systems and their components was inconsistent with documentation, as noted above, as well as with guidance.
- Regarding the remaining six systems, officials from one entity that owned two of the systems noted that those two were not included because the entity tracked its inventory separately rather than

[30] NIH officials stated, but did not provide supporting evidence, in June and July 2020 that they had included these six systems in inventory reports.

inputting the information into the agency-wide system inventory. However, NIH policy requires entities to report all of their systems to the agency. Entity officials that owned the other four systems did not elaborate on why the systems were not included.

Until NIH develops and maintains a complete and accurate inventory, OCIO and entity officials will not be able to properly manage resources to ensure the confidentiality, integrity, and availability of the agency's systems. In addition, until NIH reports a complete system inventory to OMB and DHS, those agencies lose an opportunity to provide effective oversight.

NIH Categorized Selected Systems, but One Was Not Documented in a Manner Consistent with Guidance

Categorizing information systems is a critical step in assessing risk and determining security requirements. FIPS 199 requires agencies to categorize systems based on an assessment of the potential impact of a loss of confidentiality, integrity, or availability. In assessing the impact agencies should, among other things, assess and document personally identifiable information (PII). In addition, *The E-Government Act of 2002* requires federal agencies to conduct privacy impact assessments for systems or collections containing personal information. Further, NIST guidance recommends that agencies conduct a privacy impact assessment for each system and identify if PII is on a system. NIH policy generally aligns with NIST guidance and requires entities to document each system's categorization and privacy impact assessment.

NIH had appropriately assigned FIPS 199 impact ratings to the 11 selected systems; however, one system was not documented in a manner consistent with guidance.[31] Specifically, the one GSS—a system that the agency deemed to be non-sensitive—included minor applications that had PII for individuals.[32] However, entity officials did not document the PII in system categorization documentation or the system's privacy

[31] At the time of our initial review in February 2019, the agency had not assigned one of the selected systems an impact categorization in its FIPS 199 documentation; however, the agency assessed and finalized an impact categorization in September 2019. According to NIH officials, the system had been categorized, but a lack of quality control had led to inconsistent documentation.

[32] A minor application is a non-major system that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a GSS.

impact assessment. Thus, agency officials with oversight responsibilities may not have been aware of the potential privacy impacts associated with operating the GSS.

Entity officials acknowledged that the GSS contained non-sensitive PII that had not been appropriately documented. In addition, the officials stated, but did not document in a plan or schedule, that they intend to take steps to appropriately document PII. Until NIH and its entity document the categorization of this information system in a manner consistent with guidance, the agency and entity will not have a full understanding of the potential impact that a loss of confidentiality, integrity, or availability for the system would have on organizational operations and assets, individuals, other organizations, and the nation.

NIH Developed Elements of a Risk Management Strategy and Took Steps to Determine Risk for Selected Systems, but Deficiencies Existed

FISMA requires agencies to assess the risk of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information systems. To address risk from an organizational perspective, NIST recommends that agencies develop and execute a comprehensive and agency-wide risk management strategy specific to information systems.[33] NIST also states that risk assessments are an important tool for effectively managing the risks associated with operating information systems.[34]

NIH Developed Elements of an Information System Risk Management Strategy, but Did Not Have a Comprehensive Strategy

NIST SP 800-37 recommends that agencies develop a risk management strategy associated with the operation and use of information systems. Such a strategy is to provide information system officials with, among other things, risk assessment methodologies, risk mitigation approaches, an organizational risk tolerance, and approaches for monitoring risk. NIH policy, consistent with NIST guidance, requires the agency to develop a

[33] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

[34] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30 (Gaithersburg, MD: September 2012).

risk management strategy associated with the operation and use of information systems.

NIH had taken steps to develop elements of a risk management strategy specific to the use of its information systems, but it had not developed a comprehensive strategy. For example, while the agency had developed guidance that documented its methodologies for conducting risk assessments, the agency had not developed a risk management strategy that included all the elements recommended by NIST. Specifically, NIH had not developed an information system risk management strategy that fully addressed risk mitigation approaches, organizational risk tolerance, or approaches for monitoring risk.

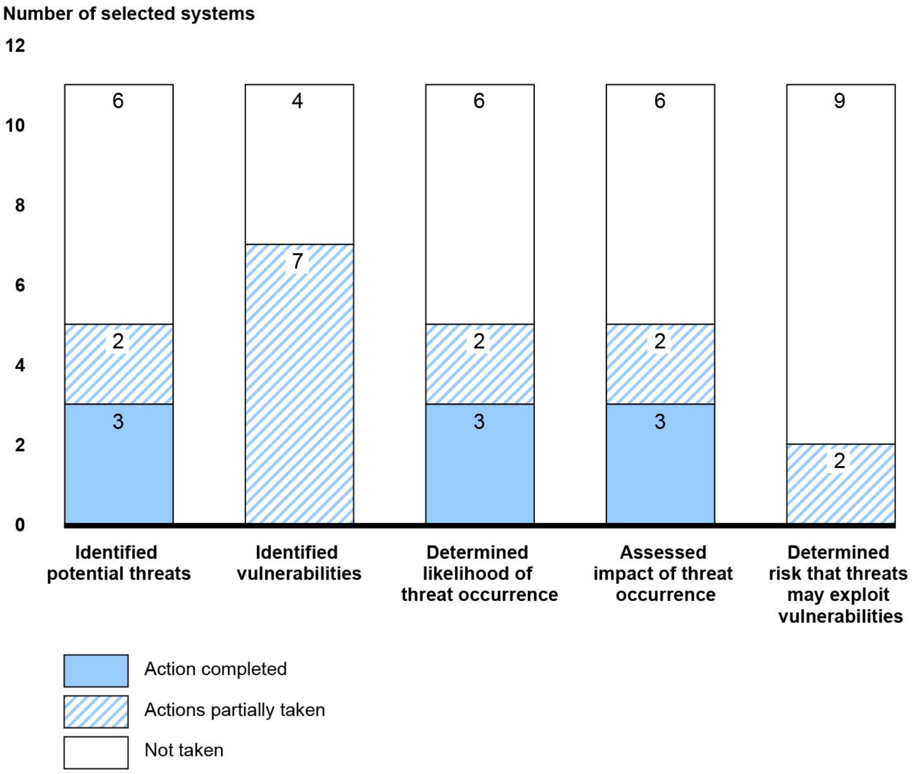
NIH officials asserted that the agency had an information system risk management strategy because they conducted activities associated with elements of a risk management strategy. Nevertheless, these activities were not guided by a comprehensive strategy that would ensure consistent implementation of risk management requirements. Moreover, until NIH fully develops such a strategy, the agency will not have guidance and relevant information needed to fully manage the risks associated with the operation of its information systems.

NIH Took Steps, but Did Not Fully Determine Risk for Any Selected Information System

NIST SP 800-37 recommends that risk assessments be conducted for each information system. Further, NIST SP 800-30 provides guidance to determine risk through five key steps: 1) identify potential threats (and associated events) to the organization and its information systems; 2) identify vulnerabilities in its systems; 3) determine the likelihood that a particular threat may exploit vulnerabilities; 4) assess the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data; and 5) determine the risk that threats may exploit vulnerabilities. NIH policy is consistent with NIST guidance and requires entity officials to conduct, document, and acknowledge system risk assessments.

However, the NIH entities in our review did not fully conduct risk assessments for the 11 selected systems. For example, the entities did not fully determine the risk that threats may exploit vulnerabilities for any of the systems. Figure 1 summarizes the extent to which the four selected entities had taken actions to address the five key steps for assessing the information security risks of the 11 selected systems, as of December 2019.

Figure 1: GAO Assessment of U.S. National Institutes of Health (NIH) Actions to Address Five Key Risk Assessment Steps for 11 Selected Information Systems in Four Selected Entities, as of December 2019



Source: GAO analysis of NIH data. | GAO-22-104467

Accessible Data Table for Figure 1

Number of selected systems	Action Completed	Actions partially taken	Not taken
Identified Potential threats	3	2	6
Identified vulnerabilities	0	7	4
Determined likelihood of threat occurrence	3	2	6
Assessed impact of threat occurrence	3	2	6
Determined risk that threats may exploit vulnerabilities	0	2	9

In addition, ISAO officials had provided risk assessment feedback to relevant officials at each of the four selected entities, but entity officials did not implement the feedback. Specifically, ISAO officials communicated to entity and OCIO officials that assessments were incomplete. However, risk assessment documentation showed that officials from all four entities had not taken steps to fully address feedback and complete the risk assessments. Further, in December 2019, OCIO officials said that risk assessments were incomplete because entity officials did not fully carry out their responsibilities or understand the requirements.

Entity officials responsible for risk assessments provided different viewpoints on why they had not fully addressed the risk assessment steps. Officials at one entity stated that they were under the impression that their security assessment reports captured risk assessments. However, the security assessment reports did not include a full assessment of risk.

Further, officials from another entity stated that their entity had not fully implemented its risk assessment process in accordance with agency guidance. For a third entity, officials stated that they were unsure why risk assessments were incomplete and added that, while they were working to improve their process, they previously did not have sufficient personnel to do so.

In a subsequent July 2020 written statement, NIH officials said that the four entities had fully conducted risk assessment activities for all selected systems. However, while additional documents showed that risk management activities had taken place, the entities had not fully conducted the five key risk assessment steps for any of the 11 selected systems. Until the selected entities conduct risk assessments for information systems in a manner consistent with guidance, these entities will not be positioned to effectively manage the risks associated with operating their systems.

NIH Had Security Plans for Selected Systems, but Did Not Fully Develop or Review Them

A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes subordinate plans for providing adequate information security for networks, facilities, and systems or a group of information systems, as appropriate.

NIST SP 800-53 and 800-18 guidance states that organizations should develop system security plans that, among other things, describe the security categorization and rationale, system boundary, inventory of primary hardware and software, system interconnections and memorandums of understanding, and security controls in place.[35] The NIST guidance also says that security control descriptions should state how the control is implemented or planned to be implemented, to include describing agency defined requirements for select security controls.

In addition, NIST SP 800-18 recommends that agencies document compensating controls if prescribed controls do not meet security requirements. Further, NIST SP 800-53 states that controls should reference guidance or additional documentation in control descriptions, as appropriate.

NIH policy was consistent with NIST guidance, and assigned responsibilities for the development of the security plan to system owners. The policy also stipulated that the plans are to be reviewed and updated at least annually, and are to be endorsed by entity CIOs.

[35] National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18 (Gaithersburg, MD: February 2006).

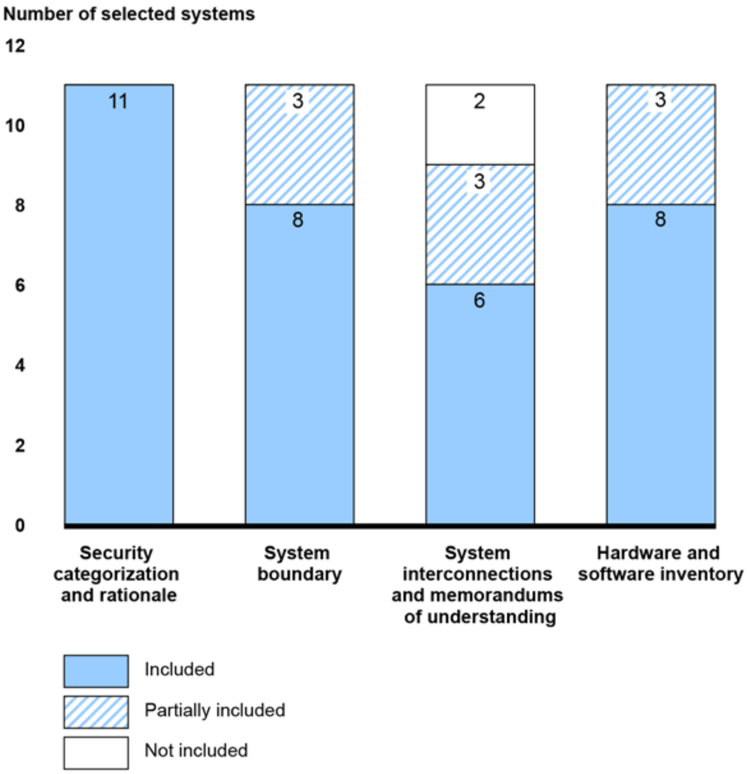
At the agency-wide level, NIH took some steps to ensure the documentation of system security plans. These steps included:

- Implementing an agency-wide security authorization management tool for entities to use in order to develop and generate consistent security plans across the agency.
- Providing templates and guidance to each of the entities. NIH officials created a security plan template to ensure all required information was accounted for when using the agency's security authorization management tool.

The selected entities took steps to develop security plans for the 11 selected systems. However, required elements of those plans, such as security categorization and rationale, system boundary, inventory of primary hardware and software, and system interconnections and memorandums of understanding, were not always consistent with recommended guidance. For example, security plans for five systems did not fully list system interconnections and memorandums of understanding. Such a listing of interconnections and memorandums is essential to document the officials' consideration of interconnection risks and control requirements.

In addition, security plans for four systems were not generated using the agency-wide authorization management tool and used incorrect or outdated templates, resulting in insufficiently documented elements such as system interconnections and inventories. Figure 2 shows the extent to which the system security plans included the required elements, as of September 2019.

Figure 2: GAO Assessment of Required Elements of Selected U.S. National Institutes of Health (NIH) Entities' System Security Plans, as of September 2019



Source: GAO analysis of NIH data. | GAO-22-104467

Accessible Data Table for Figure 2

Number of selected systems	Included	Partially included	Not included
Security categorization and rationale	11	0	0
System boundary	8	3	0
System interconnections and memorandums of understanding	6	3	2
Hardware and software inventory	8	3	0

Beyond the required elements, security plans for the 11 selected systems contained security control descriptions that identified how security controls were implemented. However, seven of the 11 security plans were missing at least one of the security controls required by NIH guidance, and all 11 security plans included incomplete and/or inaccurate security control descriptions. For example, security control descriptions often lacked agency-defined requirements and did not clearly identify individuals with critical security responsibilities. In addition, security control descriptions did not always address the intended control or inaccurately stated that security controls were in place and operating effectively when they were not. Further, security plans for the 11 selected systems did not always document compensating controls when security requirements were not met.

While NIH took some steps to reference guidance and additional documentation in selected system security plans, the agency did not do so comprehensively. For example, for one system, none of its configuration management controls referenced a configuration management plan, which provides additional details on processes and procedures, or where such information could otherwise be found.

Moreover, although entity officials had reviewed the security plans for nine of 11 selected systems on an annual basis, they had not done so for the other two systems.[36] Table 1 shows the number of examined security controls completely and accurately described in the security plans for each system and if that plan had been reviewed annually, as of September 2019.

Table 1: GAO Assessment of Security Controls in Selected U.S. National Institutes of Health (NIH) Entities' System Security Plans,* as of September 2019

	Number of examined security controls completely and accurately described in the system security plan	Security plan reviewed annually
System 1	41 of 65	Yes
System 2	12 of 65	Yes
System 3	36 of 54	Yes
System 4	32 of 54	No
System 5	56 of 65	Yes
System 6	43 of 54	Yes
System 7	47 of 65	Yes
System 8	31 of 65	Yes
System 9	14 of 54	Yes

[36] Officials stated in July 2019 that they had developed a draft version of the updated security plan for one of the systems.

System 10	10 of 54	No
System 11	27 of 29	Yes
Total of the examined security controls for the 11 selected systems	**349 of 624**	

Source: GAO analysis of NIH data. | GAO-22-104467

*To review controls for selected systems, we established a baseline of 65 controls from a population of 169 controls judged relevant to our audit work. Specifically, 58 were randomly selected and 7 were judgmentally selected. However, based on system impact level, not all controls were applicable for the moderate- and low-impact systems. We reviewed 54 controls for moderate-impact systems and 29 for the low-impact system. Across the 11 selected systems, we reviewed a total of 624 individual control assessments.

According to OCIO officials, in some cases, security plans did not meet agency standards because processes and training were not fully in place. However, OCIO officials further stated that they were working to improve their security control documentation. Nevertheless, security plans were inconsistent with policy, incomplete, and contained inaccurate security control descriptions.

In addition, regarding not having conducted a review of two security plans, OCIO officials said that they had deferred an annual review of one system and were making significant changes to the documentation and oversight of the other system. Nevertheless, both security plans had not been updated and reviewed by management in over 2 years—twice the interval required by guidance.

Until NIH takes steps to more completely develop, document, and review security plans for all selected systems, the agency increases the risk that controls are not implemented effectively and security requirements have not been met. Further, without adequately documenting security plans, agency officials are at increased risk of not possessing the information needed to understand how security controls are implemented.

NIH Authorized Operations of Systems but Deficiencies in System Boundaries and the Authorization Process Exist

NIH Authorized Operations of Systems but Two Lacked Identified Authorization Boundaries

NIST SP 800-37 recommends that agencies' federal information systems have a security authorization. A security authorization is the decision given by a senior official to put an information system into operation, based on a defined system boundary, and to explicitly accept the risk to the organization. In addition, NIST recommends that agencies explicitly define system boundaries and, thus, what makes up that system, in the system's security plan.[37] NIH policy is consistent with NIST guidance and requires documentation of system boundaries and security plans as part of its authorization process.

While NIH authorized the 11 selected systems to operate, two of those authorizations were not based on defined system boundaries. Specifically, the CISO had authorized the two systems to operate as components of two other systems (referred to as clusters). However, officials had done so without documenting system boundaries that identified the two systems as components within those clusters. For example, the agency did not develop security plans for the clusters, as required by guidance and agency policy, which would have defined system boundaries and the components that make up the clusters. Thus, it was not clear what components officials had authorized to operate or that they had accepted the associated risks to the organization.

According to OCIO officials, the clusters were not systems, rather they were, "groupings of systems" and, therefore, did not need security plans.[38] Thus, among other things, the clusters did not have defined system boundaries. Nevertheless, NIH documentation, such as the May 2019 FISMA quarterly report, identified the clusters as systems. Further, OCIO officials said the agency was in the process of establishing system authorization boundaries for these systems that better address the authorization process. However, the agency did not have any documented timelines for implementation of this process.

While guidance allows agencies flexibility in determining system boundaries, a key requirement is defining those boundaries in system security plans so officials have sufficient knowledge of what comprises those systems. Moreover, until NIH ensures that systems are authorized to operate based on defined system boundaries, the agency will not have a full understanding of the risks associated with operating the systems.

[37] NIST, SP 800-53.

[38] NIST recommendations allow for agencies to group information systems with common functions into a single system; however, these "systems of systems" are subject to the same requirements as other information systems.

Selected Entities Had Authorization Processes, but Had Not Fully Integrated Their Processes into the Agency-wide Program

NIST SP 800-53 states that, through security authorization processes, agencies should manage the security state of information systems and the environments in which those systems operate. In addition, agencies are to fully integrate the security authorization processes into an agency-wide program. NIH policy aligns with NIST requirements and further stipulates that, as part of the system authorization process, entities are to submit key documents to the NIH ISAO for oversight.[39]

To integrate the security authorization processes into an agency-wide program, NIH developed agency-wide tools and a process to review key authorization documents. Agency-wide tools included a central document repository as well as templates intended to ensure consistent entity documentation. ISAO also reviewed key documents submitted by entities and provided oversight through written feedback.

However, selected entities did not always use provided tools to integrate their authorization processes into NIH's agency-wide program. For example, officials at one entity had not used the central NIH repository to document one selected system. As a result, ISAO had not been able to provide oversight for key authorization documents. In addition, entity officials had not used documentation templates required by the agency for four of 11 selected systems, leading to incomplete key documentation. For example, required information such as impact categorizations, risk assessments, and system boundaries was not documented.

In addition, although ISAO provided written feedback on inconsistencies, entity officials did not take corrective actions for six of 11 systems. For example, ISAO provided feedback on entities' key authorization documents that noted inconsistencies with NIH policy such as outdated, inaccurate, and incomplete content. Yet, entity officials did not implement this ISAO feedback before finalizing documentation. Subsequently, NIH authorized the six systems to operate with the unremediated inconsistencies in key authorization documentation, such as impact categorizations, risk assessments, and defined system authorization boundaries.

[39] The NIH Information Security and Awareness Office manages, among other things, agency-wide information system assessment and authorization efforts.

OCIO officials stated that, while they are in constant communication with stakeholders to address gaps and implement authorization processes in accordance with federal requirements, entities did not always use agency-wide tools and templates during the authorization process for various reasons. Specifically, these officials said that the tools and templates were difficult to use, did not meet entity needs, were redundant, and staff were unfamiliar with them. Regarding entities not taking corrective actions, OCIO officials stated that the authorization processes were not fully in place and staff were not always aware of requirements.

In addition, OCIO officials stated that the CISO will authorize systems if documentation issues are not considered significant. As a result, the agency authorized systems with significant inconsistencies in documentation, and did not hold officials responsible for remediating those inconsistencies. For example, as noted previously, officials authorized six systems without documenting critical elements needed to manage and protect information resources, such as impact categorizations, risk assessments, and defined system authorization boundaries.

Until NIH takes steps to fully integrate entities into an agency-wide program for security authorization, the agency will have less assurance of the security posture for its information systems. In addition, until entity management is held accountable for remediating inaccurate and incomplete documentation, the security authorization process will likely continue to have deficiencies.

NIH Established Guidance but Did Not Completely Develop, Document, and Review Policies and Procedures

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes policies and procedures. According to NIST SP 800-53, an agency should develop policies and procedures for each of the 18 NIST security control areas to facilitate controls' implementation. Those policies should contain details addressing, among other things, purpose, scope, roles, responsibilities, management commitment, and compliance related to the controls' implementation. In addition, the agency should develop and document procedures which detail how to implement the policies. Further, HHS and NIH established requirements for the agency to review information security policies and procedures at least once every 3 years.

NIH took steps to develop, document, and review policies and some procedures that addressed each of the 18 NIST control areas, but did not fully develop, document, and review policies and procedures. For example, while the agency fully developed and documented policies for five control areas, the agency only partially developed and documented policies for the 13 other areas. Specifically, NIH's policies did not fully address the purpose, scope, roles, responsibilities, management commitment, coordination, and compliance for the 13 control areas.

In addition, the agency did not always fully develop procedures to facilitate the implementation of agency policies for 10 of 18 control areas. For example, while NIH developed procedures for control areas such as configuration management, identification and authentication, system maintenance, and media protection, the procedures did not fully detail how to implement those control areas.

Further, the agency did not always conduct reviews of policies and procedures at least once every 3 years, as required. For example, NIH had not fully reviewed either the policies or procedures within that time frame for six control areas. Table 2 shows the extent to which NIH developed, documented, and reviewed policies and procedures for the 18 control areas.

Table 2: Extent to Which the U.S. National Institutes of Health Developed, Documented, and Reviewed Policies and Procedures as Outlined by the NIST SP 800-53 Security Control Areas*

Security control area	Policy developed and documented	Procedure developed and documented	Policy reviewed within last 3 years	Procedure reviewed within last 3 years
Access control	Activity conducted	Activity conducted	Activity not conducted	Activity not conducted
Security awareness and training	Activity conducted	Activity partially conducted	Activity not conducted	Activity not conducted
Audit and accountability	Activity partially conducted	Activity conducted	Activity conducted	Activity conducted
System assessment and authorization	Activity partially conducted	Activity conducted	Activity conducted	Activity not conducted
Configuration management	Activity partially conducted	Activity partially conducted	Activity conducted	Activity not conducted
Contingency planning	Activity partially conducted	Activity conducted	Activity conducted	Activity conducted
Identification and authentication	Activity partially conducted	Activity partially conducted	Activity not conducted	Activity not conducted
Incident response	Activity conducted	Activity conducted	Activity not conducted	Activity not conducted

System maintenance	Activity partially conducted	Activity partially conducted	Activity conducted	Activity conducted
Media protection	Activity partially conducted	Activity partially conducted	Activity not conducted	Activity not conducted
Physical and environmental protection	Activity partially conducted	Activity not conducted	Activity conducted	Activity not conducted
Security planning	Activity conducted	Activity conducted	Activity conducted	Activity not conducted
Program management	Activity conducted	Activity conducted	Activity conducted	Activity conducted
Personnel security	Activity partially conducted	Activity not conducted	Activity conducted	Activity not conducted
Risk assessment	Activity partially conducted	Activity conducted	Activity conducted	Activity conducted
Services and system acquisition	Activity partially conducted	Activity not conducted	Activity conducted	Activity not conducted
System and communication protection	Activity partially conducted	Activity not conducted	Activity partially conducted	Activity not conducted
System and information integrity	Activity partially conducted	Activity not conducted	Activity conducted	Activity not conducted

Source: GAO analysis of National Institutes of Health data. | GAO-22-104467

*National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013). Revision 4 was the latest version of the publication during our review of policies and procedures.

OCIO officials believed the agency had developed policies and procedures that were generally complete for all 18 control areas, stating that they had sufficiently addressed each area. However, the agency did not fully develop policies and procedures with sufficient detail for guidance and implementation. In addition, the officials said that policies and procedures had not been consistently reviewed every 3 years as required because they had prioritized information security operations instead. Further, the officials stated that they had not fully implemented processes and training to ensure that policies and procedures were consistent with NIST recommendations. Until the agency fully develops, documents, and reviews its policies and procedures for implementing security controls, the agency will lack assurance that effective controls are in place and operating as intended.

NIH Implemented Controls to Protect Its Systems, but Numerous Deficiencies Existed

The *protect* core security function found in the NIST cybersecurity framework is intended to help agencies develop and implement the appropriate safeguards for their systems to ensure achieving agencies' missions and to support their ability to limit or contain the impact of a potential cybersecurity event.[40] This function includes implementing controls to limit access to authorized users, processes, or devices; encrypting data to protect its confidentiality and integrity; configuring devices securely and updating software to protect systems from known vulnerabilities; and providing training for cybersecurity awareness and performing security-related duties.

Although NIH had implemented controls to protect its operating environment, it did not consistently

- implement access controls effectively,
- encrypt sensitive data,
- configure devices securely or apply patches in a timely manner, and
- ensure staff with significant security responsibilities received role-based training.

NIH Had Implemented Access Controls, but Deficiencies Existed

A basic management objective for any agency is to protect the resources that support its critical operations from unauthorized access. Agencies accomplish this objective by designing and implementing controls that are intended to prevent and limit unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to identifying and authenticating users, authorizing access needed to perform job duties, protecting system boundaries, and physically protecting information system assets. NIH took steps to implement numerous access controls, but deficiencies often existed in the implementation of these and other controls.

NIH Used Authentication Controls for Information Systems, but Did Not Fully Implement the Controls

Identification is the process of distinguishing one user from all others. Authentication is the process of determining whether individuals are who they say they are. Specifically, multifactor authentication in computer networks involves using two or more factors to ascertain authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification

[40] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

and authentication—such as user account-password combinations—provides the basis for establishing accountability and for controlling access to IT systems.

NIST SP 800-53 recommends that organizations establish password management controls for information systems such as, among other things, minimum password complexity requirements. In addition, NIST guidance recommends that organizations set defined limits on consecutive failed login attempts over a defined time period. NIST guidance also states that centralized password management can help organizations reduce the number of account identifiers and passwords that users need to remember. NIH policy specified password requirements such as a minimum of eight characters and use of upper and lowercase characters, as well as special and numeric characters. NIH policy also defined a limit of five failed login attempts within 120 minutes.

Further, NIST guidance recommends that organizations implement multifactor authentication for network access to privileged and non-privileged accounts. Microsoft also recommends that domain controller administrator accounts be restricted to only log into the domain controllers and only be accessed through a dedicated workstation whose sole purpose is to access the domain controllers in order to mitigate credential theft techniques.[41]

NIH took steps to implement strong password and authentication settings among their servers and devices. For example, NIH had implemented appropriate password settings on operating systems and applications. However, strong password management settings were absent from a number of NIH servers and devices.

OCIO officials stated that the reason the agency had not fully implemented identification and authentication controls was because doing so could negatively impact system functionality or business needs. However, the officials did not elaborate on how implementing those controls, such as password length and complexity requirements, would impact functionality or business needs. In addition, OCIO officials did not demonstrate that they had documented and accepted the risk of not implementing these requirements. Further, the officials speculated, but

[41] Domain controllers are servers that control an organization’s user identification and authentication functions.

did not demonstrate or document, that there may have been constraints or conflicts due to the complexity and scale of NIH's federated environment.

Until NIH applies more restrictive authentication methods on key information systems, NIH systems are at an increased risk of compromise and credential theft. Moreover, less restrictive authentication could lead to a variety of exploits from advanced persistent threats, including attackers gaining administrative privileges.

NIH Reviewed Privileged Accounts, but Reviews Were Incomplete and Inconsistent with NIH Policy

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information that grants a user only those access rights and permissions needed to perform official duties and minimizes the number of privileged users and limits functions that can be performed when using privileged accounts.

To avoid unintentionally authorizing user access to sensitive files and directories, an agency must carefully consider its assignment of rights and permissions. NIST SP 800-53 and NIH policy state that agencies should employ the principle of least privilege by conducting privileged user account reviews.[42] In addition, NIST SP 800-53 and NIH policy provided definitions to support consistent user reviews. Specifically, NIH policy defines a privileged account as one with the authorizations of a privileged user, and defines a secondary account as an alternate account to a user's primary account intended to provide administrative privileges to that person.[43] To support processes such as the review of user

[42] NIST and NIH define a privileged user as one that is authorized to perform security-relevant functions that ordinary users are not authorized to perform.

[43] Administrative functions are those that may be security-relevant, and are not granted to regular users; users with access to administrative secondary account functions are privileged users.

accounts, *Standards for Internal Control in the Federal Government* state that agencies should use quality information to achieve their objectives.[44]

NIH has taken steps to employ the principle of least privilege. Specifically, NIH reviewed the majority of privileged users on its network, and established agency-wide records of review to track the status of privileged user review efforts. However, the four selected entities had not reviewed all privileged user accounts in a manner consistent with policy. For example, based on a generalizable random sample of privileged users, three entities could not demonstrate that they had reviewed an estimated 10 percent of privileged users.[45]

In addition, NIH's privileged user account reviews did not use quality information, as the privileged user account review data were incomplete and inconsistent. The entities also inconsistently interpreted NIH policy. For example, some entity officials noted that they did not necessarily consider secondary accounts to have privileged access, although NIH policy defines secondary accounts as accounts used to provide users with privileged access.

Nevertheless, NIH officials asserted that the agency had validated all privileged user accounts. After our initial fieldwork, NIH provided additional user information to support their position. However, our review of this additional information validated our original finding of significant problems with the review process.

Until NIH conducts a complete privileged user review—including users with secondary accounts—the agency is at an increased risk that users may have more access than required. Moreover, until the three entities implement agency policy, the agency is at risk that privileged user access may not be reviewed consistently.

NIH Had Enabled Excessive Permissions for Servers and Databases

NIST SP 800-53 and NIH policy state that agencies should employ the principle of least privilege, providing users (or processes acting on behalf of users) the least amount of authorized access necessary to accomplish

[44] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, (Washington, DC: Sept. 10, 2014).

[45] The fourth entity provided documentation that privileged user reviews took place, but not in sufficient detail to determine the entity's effectiveness.

assigned tasks. Least privilege can be achieved by implementing restrictive access permissions that provide users with no more than the minimum amount of access required to complete their job responsibilities.

NIH took steps to implement user access controls to employ the principle of least privilege. However, NIH granted excessive permissions to users across a variety of agency servers and databases.

According to OCIO officials, the primary reason the agency had not fully implemented restrictive access permissions was that their implementation caused problems with functionality or business needs. However, NIH did not demonstrate that they accepted and documented the risk of unimplemented requirements. In addition, OCIO officials stated, but did not document or demonstrate, that there may have been operational constraints or conflicts due to the complexity and scale of NIH's federated environment. Nevertheless, unless NIH takes steps to limit excessive permissions on their networks and databases, the agency remains at an increased risk of exposure and compromise, and is highly vulnerable to privileged escalation attacks.

NIH Effectively Implemented Some, but Not All, Boundary Controls to Ensure Network Integrity

Network boundary controls are key aspects of protecting network integrity within federal agencies. To ensure that network boundaries are properly protected, agencies should establish security controls of logical connections via networks and devices. Implementing multiple layers of security, such as firewalls and network monitoring software, to protect an information system's boundaries can reduce the risk of a successful cyberattack. Specifically, firewalls can be used as part of networks to protect external boundaries and key internal boundaries within a system.

NIST SP 800-53 states that agencies should control communications at information systems' external boundaries and key internal boundaries. It states that, to manage risks, agencies should use boundary protection mechanisms to separate or partition computing systems and network infrastructures. In addition, National Security Agency guidance recommends securing and managing network devices to prevent lateral movement and privilege escalation in the event that a server is compromised.[46]

Although NIH had implemented controls, such as layered security controls that were designed to protect system boundaries, the agency had not sufficiently restricted external network traffic from accessing internal networks and systems.

OCIO officials provided various possible reasons for insufficiently restricting traffic. These officials stated that there may have been operational constraints or conflicts in implementing boundary controls due to the complexity and scale of NIH's technical environment. However, NIH did not document or demonstrate these constraints or conflicts. In addition, OCIO officials said that the agency had not fully implemented boundary controls because doing so could cause problems with functionality or business needs.

However, the officials did not elaborate on how implementing boundary controls would impact functions and business needs. Moreover, NIH did not demonstrate that the agency had accepted and documented the risk of unimplemented requirements. Without stronger boundary controls, NIH is at risk that an attack could exploit these deficiencies and compromise NIH's internal network.

NIH Took Steps to Ensure Physical Security, but Some Facilities Did Not Monitor Access

Physical and environmental security controls are key measures taken by an agency to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. NIST SP 800-53 recommends that agencies implement physical access controls by securing information system network infrastructure as well as output devices. Facilities should have adequate power, fire, and water damage protection. NIST further states that agencies should control ingress/egress access to facilities as well as securing keys and other physical access devices. It also states that agencies should monitor facilities, to include physical intrusion alarms and surveillance. In addition, NIST stipulates that agencies are to maintain visitor access records for facilities where each information system resides. High-impact systems

[46] National Security Agency, *The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)*, (Fort Meade, MD: May 15, 2006).

are further required to employ automated mechanisms to facilitate the review of visitor access records.

NIH took several actions to secure the eight facilities we reviewed that contained hardware such as servers and network infrastructure for the 11 selected information systems. All facilities secured the network infrastructure, such as cabling and switches, and had adequate power, fire, and water damage protection safety measures; however, some did not implement all required physical access controls. For example, three facilities had not fully implemented monitoring controls and four had not fully implemented automated reviews of visitor records.

Officials at one entity stated that they were in the process of upgrading one of the data centers, while officials at another entity cited other compensating controls. However, they did not explain or document how these controls effectively compensated for identified deficiencies.

Until NIH takes steps to ensure that all facilities have secure entry/exit points and access monitoring in place, and that facilities with high-impact systems have automated maintenance and review of visitor records, the agency's data facilities are at increased risk that a threat may physically access systems.

NIH Took Steps to Encrypt Sensitive Data, but These Actions Were Not Always Consistent with Guidance

Protecting the confidentiality and/or integrity of organizational information can be accomplished by logical means such as employing encryption techniques. NIST SP 800-53 states that agencies must encrypt authentication information both while stored and in transmission, and configure information systems to establish a trusted communication path between the user and the system. In addition, NIST requires that, when agencies use encryption, they use an encryption algorithm that complies with FIPS 140-2.[47]

NIH used FIPS-compliant encryption for some network devices and firewalls but did not effectively implement encryption controls in other areas. OCIO officials provided various possible reasons that the agency did not fully implement encryption consistent with guidance. According to

[47] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2 (Gaithersburg, MD: May 25, 2001).

these officials, the primary reason the agency had not fully implemented encryption controls was that their implementation could cause problems with functionality or business needs. In addition, OCIO officials stated that there may have been operational constraints or conflicts due to the complexity and scale of NIH's federated environment. However, NIH did not document or demonstrate these constraints or conflicts. In addition, the officials did not demonstrate that they had accepted and documented the risk of unimplemented requirements.

Unless NIH takes steps to further implement encryption controls, agency hardware and software may be more exposed to breaches of information that may compromise the confidentiality, integrity, and availability of sensitive information. Further, a lack of proper encryption controls may lead to breaches becoming more potent due to clear-text information and credentials being available to an attacker.

NIH Took Steps to Configure Servers Securely and Applied Patches, but Had Not Done So in a Consistent and Timely Manner

Configuration management controls are intended to provide reasonable assurance that systems are configured and operating securely and as intended. According to NIST, configuration settings are the set of parameters that can be changed in system components that affect the security posture and/or functionality of the system. Patch management, a component of configuration management, is an important element in mitigating the risks associated with known vulnerabilities. When vulnerabilities are discovered, the vendor may release an update, called a patch, to mitigate the risk. Unless the patch is applied in a timely manner, an attacker may exploit a vulnerability not yet mitigated, enabling unauthorized access to information systems or enabling users to have access to greater privileges than authorized.

NIST SP 800-53 states that agencies should disable certain services with known security vulnerabilities. This includes configuring security baselines in accordance with publicly available operating systems' security checklists (or benchmarks) promulgated by NIST's National Checklist Program repository, such as the Center for Internet Security

Windows Security baseline standards.[48] Further, NIST SP 800-53 recommends that organizations promptly test and install newly-released security patches, service packs, and hot fixes. Moreover, NIH policy states that the timeline to remediate critical vulnerabilities is within 30 days, high within 60 days, and medium and low within one year.

NIH had documented security configuration baselines, but did not always securely configure its systems or apply patches. For example:

- The agency did not consistently configure security baselines in accordance with the standards.
- NIH had not installed 26 updates since September 2016 on 175 network devices.

According to NIH, the primary reason the agency had not fully configured systems in accordance with guidance and applied patches was that doing so would cause problems with functionality or business needs. However, NIH did not demonstrate that they accepted and documented the risk of unimplemented requirements. In addition, OCIO officials stated that there may have been operational constraints or conflicts due to the complexity and scale of NIH's federated environment. However, NIH did not document or demonstrate these constraints or conflicts. Further, by not securely configuring systems and applying patches in a timely manner, the agency is at increased risk that individuals could exploit known vulnerabilities to gain unauthorized access to its computing resources.

NIH Took Steps to Ensure Personnel Completed Annual Security Awareness and Role-Based Training, but Shortcomings Existed

Personnel are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing sufficient training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. In addition, role-based training helps ensure that individuals with significant security responsibilities carry out their jobs in a manner that protects the systems involved with their job duties. However, we identified deficiencies in NIH's efforts to provide

[48] The National Checklist Program is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting the security configuration of operating systems and applications. National Institute for Standards and Technology, National Checklist Program, nvd.nist.gov/ncp/repository, (Gaithersburg, MD: n.d.).

information security awareness training to its personnel and to ensure the completion of role-based training by personnel with significant information security responsibilities.

NIH Provided Annual Security Awareness Training to Most Users, but Some Efforts Were Not Verifiable

FISMA requires that agency information security programs include security awareness training to inform personnel of the security risks associated with carrying out their responsibilities. NIST SP 800-53 recommends that information system users receive information security awareness training with a frequency defined by the agency. Consistent with NIST guidance, NIH policy requires information system users to receive annual security awareness training.

NIH took several steps to provide adequate agency-wide information security awareness training, led by the Information Security and Awareness Office. NIH delegated responsibility for ensuring that entity personnel comply with information security awareness training requirements to entity CIOs and ISSOs.

However, NIH did not effectively verify that all information system users completed required information security awareness training. Specifically, NIH training records indicated that 4,456 of 16,925 personnel from the four selected entities had not completed security awareness training as of April 2019.[49]

After our initial fieldwork, NIH provided additional user information in June 2020 regarding completion of security awareness training. However, our review of this additional information showed that NIH could not fully verify that personnel had completed training because data were inconsistent. For example, NIH indicated that some personnel did not need to complete training because they did not access information systems. Yet other records showed that many of these personnel had NIH email addresses.

OCIO officials stated that every individual provided with access to information system resources was required to take security awareness training. The officials also said there were management, technical, and administrative controls that would prevent new personnel from obtaining an account until they had taken the annual awareness training.

[49] NIH personnel include employees, fellows, contractors, guests, volunteers, and tenants.

Nevertheless, as noted above, NIH was unable to verify that all personnel had completed the annual security awareness training. Until NIH ensures that all personnel who access information systems complete annual security awareness training, users may not be informed of the information security risks associated with carrying out their responsibilities.

NIH Did Not Ensure That Personnel with Security Responsibilities Took Role-based Training

NIST requires agencies to provide role-based training to personnel with significant responsibilities for information security. According to NIST SP 800-53, adequate security training should be provided to system and network administrators and personnel conducting configuration management and auditing activities, tailoring the training to their specific roles. NIH policy also requires that personnel with significant security responsibilities receive role-based training annually.[50]

NIH had a plan in place to provide role-based training annually to the majority of personnel with significant security responsibilities. However, the agency did not ensure that training was completed consistent with agency guidance. Specifically, NIH role-based training records indicated that 549 of 2,135 personnel from the four selected entities had not completed training within the recommended defined frequency, as specified in agency policy. After our initial fieldwork, NIH provided additional user information. However, our review of this additional information validated our original finding that personnel did not complete the required annual training.

According to agency officials, personnel did not meet role-based training requirements because the agency had not fully automated its training records to identify and track individuals that required training. Agency training specialists also stated that, for many staff with information security responsibilities, the agency still managed role-based training manually, which was resource intensive. In addition, within the training system, it was difficult to determine when an individual was no longer considered to have significant security responsibilities and, thus, role-based training was no longer required.

Nevertheless, until the agency has a process in place to ensure that all personnel with significant information security responsibilities have

[50] NIH policy requires role-based training annually; however, prior to July 2018, training was required once within every 3 years.

completed role-based training requirements, personnel are at risk they will not meet requirements. Accordingly, the agency is at increased risk that staff may not have the knowledge or skills needed to appropriately protect systems.

NIH Had Implemented Controls Intended to Detect Incidents and Deficiencies, but Not All Controls Were Effective

The *detect* core security function in the NIST cybersecurity framework is intended to allow for the timely discovery of cybersecurity events.[51] Controls associated with this function include logging and monitoring system activities and configurations, assessing security controls in place, and implementing continuous monitoring. Although NIH had implemented controls intended to detect the occurrence of a cybersecurity event, it did not effectively

- implement logging and monitoring capabilities,
- comprehensively and reliably assess security controls, and
- fully implement an information system continuous monitoring program.

NIH Had Implemented Logging and Monitoring Capabilities, but Capability Weaknesses Limited Effectiveness

Logging and monitoring involve the regular collection and monitoring of security events for indications of inappropriate or unusual activity. To establish individual accountability, monitor compliance with security policies, and investigate security events, agencies need to determine what, when, and by whom specific actions have been taken on a system.

NIST SP 800-53 states that agencies should enable system-logging features and retain sufficient audit logs to support the monitoring for significant security-related events and investigations of security incidents. In addition, National Archives and Records Administration records

[51] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

retention guidance states that security incident data needed for audit or investigative purposes should be retained for at least 3 years.[52]

NIST SP 800-53 also recommends that organizations establish automated mechanisms that collect and analyze data for increased threat and situational awareness. This includes an automated centralized logging analysis capability such as from security information and event management (SIEM) technologies that can produce real-time alerts, notifications, and follow-up of significant security events generated by information systems.[53] Further, NIST and an industry leading practice recommend that organizations increase their situational awareness through boundary and internal network traffic monitoring capabilities to identify inappropriate or unusual activity.[54]

NIH took steps to implement system logging, centralized logging and analysis, and network traffic monitoring capabilities for three reviewed entities, but the capabilities were limited. For instance, the agency had not implemented system logging on certain servers, network devices, and workstations. In addition, entities did not always configure system logging to capture more details. The agency also had not fully configured its SIEM to centrally collect complete information to identify potential threat activity. Further, the agency retained only 6 months of SIEM data, instead of for at least 3 years, as required by guidance. Moreover, entities had not fully implemented network traffic monitoring capabilities.

According to OCIO officials, NIH continues to make technical improvements to address audit and monitoring issues. OCIO officials explained that the conditions we noted were caused by unfulfilled plans to address NIH's monitoring capabilities, in which significant effort was underway but not yet completed as of July 2020. The officials also stated that the ability to make technical improvements without impeding scientific activities or other significant operational activities was an issue, as were

[52] National Archives and Records Administration, *General Records Schedule 3.2: Information Systems Security Records*, Transmittal 26, (Washington, D.C.: September 2016). Agencies are to keep incident handling, reporting, and follow-up records for 3 years after all necessary follow-up actions have been completed.

[53] Security information and event management (SIEM) relates to software products and services that combine security information and event management for all enterprise systems and applications into a central data repository for real-time analysis of security alerts generated by network hardware and applications.

[54] Cisco, *Network as a Security Sensor: Threat Defense with Full NetFlow*, White Paper (San Jose, CA: Oct. 26, 2018).

operational constraints or conflicts due to the scale and complexity of NIH's federated environment. However, the agency did not demonstrate that it had accepted and documented the risk of unimplemented requirements.

Without effective logging and monitoring capabilities in place, NIH faces an increased risk that its entities will not be aware of performance issues and suspicious activity regarding unauthorized access attempts and changes to network routing, firewall, or server configurations.

NIH Assessed Controls, but Shortcomings Existed

An organization can detect whether policies, procedures, and controls are effective and operating as intended by periodically assessing them. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. Periodic testing and evaluation are to be performed with a frequency depending on risk, but no less than annually. Further, according to NIST SP 800-53A, the process may be conducted by independent assessors to provide confidence that the assessment results produced are sound and can be used to support a risk-based decision.[55]

NIST SP 800-53 recommends that agencies assess security controls to determine the extent to which the controls have been implemented correctly and are operating as intended. NIST recommends agencies base determinations on test results that are specific to the control and supported by evidence.

NIH's policy aligned with NIST guidance, and also established the role of the independent security control assessor with responsibility for assessing controls and reporting the results of assessments to entity CIOs, system owners, and ISSOs. Further, NIH policy defined an annual frequency of review which consists of approximately one-third of the security controls, such that an entire set of security controls is reviewed within every 3 years.

[55] National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Special Publication 800-53A, Revision 4 (Gaithersburg, MD: December 2014).

The agency developed a process for assessing its information security controls to determine the extent to which the controls have been implemented correctly and are operating as intended. For example, security control assessors specific to each entity conducted security control assessments and reported assessment results to entity CIOs, system owners, and ISSOs. NIH ISAO officials also reviewed assessments as part of the system authorization process.

However, entities did not fully detect control deficiencies. Specifically, the agency did not consistently 1) determine the extent to which controls had been implemented; 2) conduct assessments within required frequencies; and 3) ensure that assessors were independent. For example, the agency determined the extent of implementation for only 35 percent of assessed controls.[56] The agency had not determined the extent of implementation for the remaining 65 percent of assessed controls because they, among other things,

- lacked critical data such as test results;
- did not assess the control; or
- lacked evidence supporting the assessment result.

NIH also took steps to review and assess security controls within agency-defined frequencies for seven of 11 selected systems, but not for the four other systems. Table 3 shows the number of selected control assessments that determined the extent and effectiveness of implementation and the assessment frequencies for selected systems as of July 2019.

[56] To review specific control assessments for selected systems, we established a baseline of 65 controls from a population of 169 controls judged relevant to our audit work. Specifically, 58 were randomly selected and 7 were judgmentally selected. However, based on system impact level, not all controls were applicable for the moderate- and low-impact systems. We reviewed 54 controls for moderate-impact systems and 29 for the low-impact system. Across the 11 selected systems, we reviewed a total of 624 individual control assessments.

Table 3: GAO Assessment of U.S. National Institutes of Health (NIH) Control Assessments for 11 Selected Systems as of July 2019

System	Number of examined control assessments that determined the extent to which the controls had been implemented[a]	Controls assessed annually, and all security controls reviewed within every 3 years?
System 1	18 of 65	No
System 2	32 of 65	Yes
System 3	46 of 54	Yes
System 4	34 of 54	No
System 5	20 of 65	Yes
System 6	24 of 54	No
System 7	33 of 65	Yes
System 8	0 of 65	Yes
System 9	2 of 54	Yes
System 10	0 of 54	No
System 11	8 of 29	Yes
Total of the examined control assessments for the 11 selected systems	**217 of 624**	

Source: GAO analysis of NIH data. | GAO-22-104467

[a]Notes: To review specific control assessments for selected systems, we established a baseline of 65 controls from a population of 169 controls judged relevant to our audit work. Specifically, 58 were randomly selected and 7 were judgmentally selected. However, based on system impact level, not all controls were applicable for the moderate- and low-impact systems. We reviewed 54 controls for moderate-impact systems and 29 for the low-impact system. Across the 11 selected systems, we reviewed a total of 624 individual control assessments.

In addition, NIH did not ensure that security control assessors were independent and capable of conducting an impartial assessment of security controls at two selected entities. Specifically, the security control assessors within two selected entities not only documented controls in system security plans, but also assessed the controls and reported that the controls were adequately assessed. Given this, there is less assurance of the independence and impartiality of the security control assessments for these two entities.

OCIO officials stated in July 2020 that the agency had conducted assessments that were complete, accurate, and consistent with policy. However, the officials did not provide evidence showing this. In addition, according to OCIO and entity officials, control assessments appeared not to determine the extent of control implementation because of insufficient documentation. Nevertheless, as noted above, the agency did not demonstrate that control assessments determined the extent of implementation. Officials provided several additional reasons, in interviews from June 2019 to July 2020, why the agency was not able to fully detect control deficiencies:

- OCIO officials stated that their current processes were not mature, due to gaps in security control assessor training and quality control, but planned to improve the control assessment process across the agency.
- OCIO officials noted that two entities were comprehensively restructuring their information systems, which affected the entities' abilities to conduct assessments.
- Officials from two entities stated that they had not been involved enough in the assessment process.
- Regarding the independence of assessors, OCIO officials said that processes and training were not fully in place to ensure required independence.

Unless entities takes actions to improve assessments of security controls, the agency will continue to be unable to fully detect technical and program management deficiencies. Specifically, until NIH takes steps to (1) fully assess the extent of control implementation; (2) assess controls within required frequencies; and (3) ensure that assessors are independent, the agency will not have the assurance that security controls are effective and operating as intended.

NIH Did Not Fully Implement Continuous Monitoring Prior to Implementing Ongoing Authorization

Continuous monitoring is the continuing awareness of information security, vulnerabilities, and threats to support risk management decisions and ongoing authorization. NIST and HHS set forth continuous monitoring requirements, and NIH developed a strategy in March 2019 that aligned with those requirements. In addition, the agency's strategy established seven functional areas, such as assessment and authorization, required for continuous monitoring implementation.[57]

[57] Per the *NIH Information System Continuous Monitoring Strategy*, continuous monitoring consists of seven functional areas: policy; training and awareness; vulnerability management; continuous diagnostics and mitigation; threat mitigation and incident response; assessment and authorization; and data analysis and reporting.

According to NIST, ongoing authorization is a dynamic and cost-effective process in which an agency maintains sufficient knowledge of the security state of information systems to determine whether continued operation is acceptable based on ongoing risk determinations. While NIST SP 800-53 recommends that agencies re-authorize systems within a regular frequency, systems with an ongoing authorization do not need to be re-authorized. NIST and HHS require agencies to have an information security continuous monitoring program in place prior to an agency's implementation of ongoing authorization.[58]

While NIH took steps to develop a continuous monitoring program, the agency had only partially implemented each of the seven continuous monitoring functional areas established in guidance. For example, the agency had not fully implemented the assessment and authorization functional area. Specifically, as noted previously in this report, agency assessments were not able to fully detect deficiencies. In addition, agency officials stated that, as of April 2019, the agency had not fully implemented continuous monitoring. In subsequently provided evidence, NIH described the tools used for continuous monitoring, but did not provide evidence of the tools' implementation or effectiveness.

Further, agency documentation such as security plans, FISMA quarterly reports, and information security priority action reports noted functional area deficiencies. For example, the agency noted in its FISMA reports that data analysis and reporting was not fully implemented. Security plans also noted that vulnerability management controls had not been fully implemented for six of 11 selected systems. In addition, security priority actions reports indicated that the agency needed to take additional steps to fully implement vulnerability management and continuous diagnostics and mitigation.

NIH officials stated, in July 2020, that the agency had fully implemented a continuous monitoring program. Nevertheless, the agency had not demonstrated that it had fully implemented its program or remediated the deficiencies noted above. Until NIH takes steps to fully address deficiencies in continuous monitoring functional areas, the agency will have less ongoing awareness of information security, vulnerabilities, and threats.

[58] NIST SP 800-37 and Department of Health and Human Services, *HHS Information Security Continuous Monitoring Strategy*, (Washington, D.C.: May 2017).

Further, one selected entity implemented ongoing authorization without first ensuring that a continuous monitoring program was fully in place. Specifically, the entity had operated one selected system under ongoing authorization since December 2017 without a continuous monitoring program fully in place. Thus, officials did not have sufficient knowledge of the security posture of the system to determine whether continued operation was acceptable based on ongoing risk.

NIH officials noted that the implementation of ongoing authorization for the selected system was part of the agency's efforts to test and evaluate how to best transition to ongoing authorization. However, NIH did not demonstrate that it had evaluated or tested the transition to ongoing authorization. In addition, entity officials stated that continuous monitoring policy had allowed them to operate the system under ongoing authorization. However, the agency developed this guidance over a year after the system started operating under ongoing authorization. Further, officials did not elaborate on how policy allowed for ongoing authorization without first implementing continuous monitoring as required by NIST and HHS. As a result of the entity's operation of the system under an ongoing authorization without a continuous monitoring program fully in place, officials may not have had sufficient knowledge when making risk determinations.

NIH Had Implemented Processes for Incident Response, but Lacked Sufficient Testing, Training, Documentation, and Timely Corrective Actions

The *respond* core security function in the NIST cybersecurity framework is intended to support the ability to contain the impact of a potential cybersecurity event.[59] Controls associated with this function include implementing an incident response capability and remediating newly identified deficiencies. Although NIH had implemented controls for incident response to detect cybersecurity events, it did not always develop incident response plans and test response capability, and consistently document and take timely corrective actions to remediate identified deficiencies.

[59] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

NIH Implemented an Incident Program, but Lacked Sufficient Testing and Training, and Did Not Maintain Adequate Incident Information

Even with strong information security controls, incidents can still occur. Agencies can reduce the risks associated with these incidents by detecting them and promptly responding before significant damage is done. FISMA requires that agencies develop, document, and implement an agency-wide information security program that includes procedures for detecting, reporting, and responding to security incidents.

NIH Established a Policy, but Did Not Fully Develop Plans or Conduct Testing and Training

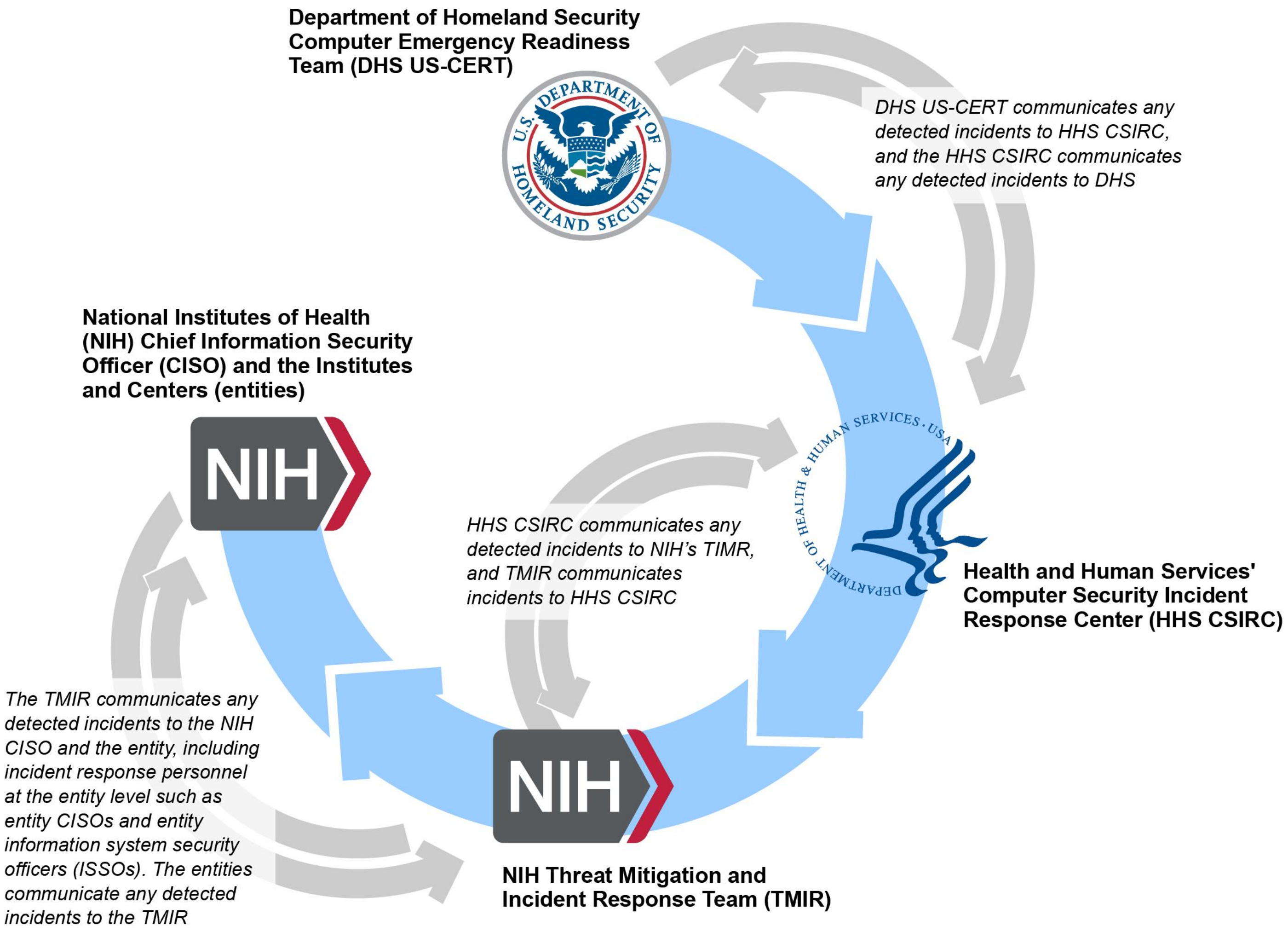
NIST SP 800-53 and SP 800-61 state that agencies should develop and document an incident response policy with corresponding implementation procedures and an incident response plan that describes the procedures, points of contact, and roles and responsibilities of individuals with significant security responsibilities.[60] NIST also states that agencies should implement an incident handling capability, including an incident response team that consists of forensic/malicious code analysts. In addition, agencies are to provide incident response training for the team, and test the incident response capability to determine the effectiveness of the response. NIH policy generally aligns with NIST requirements, and further stipulates that incident response training and testing occur at least annually. Agency policy also requires that at least a table-top incident response exercise be performed annually for moderate- and high-impact systems.

NIH developed policy and procedures, and took steps to develop and annually update plans that addressed incident response. In addition, NIH took steps to implement an incident response capability that included the development and testing of incident response plans, annual incident response training, and conducting penetration testing exercises. The agency also established the Threat Mitigation and Incident Response (TMIR) team that managed the incident response efforts for the agency, and conducted forensic analyses for reported security incidents. The team coordinates with entities and HHS' Computer Security Incident

[60] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2 (Gaithersburg, MD: August 2012).

Response Center to communicate detected cyber incidents to entities.[61] Figure 3 illustrates this process.

Figure 3: Process Used by NIH, HHS, and DHS to Coordinate on Information Security Incidents


Department of Homeland Security
Computer Emergency Readiness
Team (DHS US-CERT)
DHS US-CERT communicates any detected incidents to HHS CSIRC, and the HHS CSIRC communicates any detected incidents to DHS
National Institutes of Health (NIH) Chief Information Security Officer (CISO) and the Institutes and Centers (entities)
NIH
HHS CSIRC communicates any detected incidents to NIH's TIMR, and TMIR communicates incidents to HHS CSIRC
Health and Human Services' Computer Security Incident Response Center (HHS CSIRC)
The TMIR communicates any detected incidents to the NIH CISO and the entity, including incident response personnel at the entity level such as entity CISOs and entity information system security officers (ISSOs). The entities communicate any detected incidents to the TMIR
NIH
NIH Threat Mitigation and Incident Response Team (TMIR)

Source: GAO analysis of NIH data. | GAO-22-104467

[61] The Threat Mitigation and Incident Response team NIH-wide responsibilities include, but are not limited to: 1) maintaining security situational awareness and determining an overall IT security risk posture; 2) coordinating cybersecurity information; 3) sharing, analysis, and response activities; 4) reporting IT security and privacy incidents to HHS Computer Security Incident Response Center (CSIRC); and 5) serving as NIH's main point of contact with HHS CSIRC.

However, although the agency had taken steps in implementing its incident response capability, efforts to develop and test incident response plans and conduct incident response training were insufficient for selected systems. For example:

- Plans for two systems were missing critical information, such as key points of contact and another system did not have a plan.
- Entities had not conducted annual incident response training for five of the 11 systems.
- Entity staff had not conducted annual incident response testing for five of the 11 systems.

According to entity officials, incident response planning development, training, and testing were not always consistent with requirements because the entities did not always implement NIH agency-wide tools and feedback. Further, officials from one entity stated that the selected system utilized another system's incident response plan. However, the incident response plan for the other system did not contain plan elements, such as points of contact for staff of the selected system.

In addition, OCIO officials stated that personnel satisfied incident response training requirements through taking the annual security awareness training, and augmented that training with incident response testing conducted at the system level. However, while annual security awareness training provides basic information on the topic that is applicable to all staff, it does not address key documents and procedures associated with the incident response process. Moreover, although NIH policy permits incident response testing to satisfy training requirements, NIH had performed the tests for only five of the 10 systems that had requirements for incident response testing.

Without effectively developing and testing incident response plans, and training for the use of the plans, NIH may not be able to respond to incidents in a sufficient and timely manner. Therefore, the agency does not have assurance that it can mitigate risks associated with such incidents before substantial damage is done.

NIH Collected Incident Data, but Did Not Fully Maintain Information to Support Incident Response Capabilities

NIST SP 800-53 states that agencies should establish enhanced monitoring capabilities that include automated mechanisms to collect, analyze, and document information system security incidents. For example, this includes maintaining records about each incident, the status of the incident, and all relevant information captured on the incident that is relevant to a forensics examination. In addition, to support incident response capabilities, NIST SP 800-86 recommends implementation of enhanced monitoring capabilities, including network forensics of digital data, such as packet capture and network flow session.[62]

NIH took several steps to collect, analyze, and document information system security incidents. For example, the agency demonstrated the ability to collect data to support incident response capabilities, such as forensic system images from compromised servers and computers. Additionally, NIH incident response teams implemented tools and analyzed data from enhanced monitoring capabilities, including network data such as packet capture and network flow session data.

However, shortcomings existed with NIH's collection, analysis, and documentation of information systems security incidents. For example, among the 10 security incidents NIH considered most significant from January 2018 to February 2019:

- For two incidents, NIH failed to collect and analyze data that may have been related to the incidents prior to the remediation and reimaging of systems, resulting in the loss of data and artifacts.
- The agency did not collect key data or document analyses for two incidents.
- The agency did not document key analysis for an incident that impacted 102 user workstations across 22 institutes. Instead, the documentation focused on recovery and remediation efforts.

NIH OCIO officials said that the primary reason the agency had not fully collected, analyzed, and documented security incidents was that completely implementing the process could affect system functionality or business needs. However, the agency did not demonstrate that it accepted and documented the risk of unimplemented requirements. In addition, these officials stated, but did not demonstrate, that there may have been constraints due to the complexity and size of the federated agency. Nevertheless, maintaining adequate information to support

[62] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response*, Special Publication 800-86 (Gaithersburg, MD: August, 2006).

incident response would reduce impacts from the potential loss of confidentiality, integrity, or availability.

Without effective collection, analysis, and documentation of information system security incidents, the agency's ability to respond to incidents is limited. In addition, NIH is limited in its ability to determine root cause, develop accurate and complete detailed timelines, and apply lessons learned in preventing future incidents.

NIH Remedial Action Plans Addressed Deficiencies for Selected Systems, but Did Not Always Contain Sufficient Detail or Lead to Timely Corrective Actions

FISMA requires each agency to document remedial actions to address any deficiencies in information security policies, procedures, or practices. OMB and NIST state that agencies should develop plans of action and milestones (POA&Ms) to assist agencies in identifying, assessing, prioritizing, and reporting on the progress of corrective efforts.

POA&Ms Did Not Always Contain Sufficient Detail and NIH Did Not Consistently Track Them

NIST SP 800-53 states that agencies should develop POA&Ms to document planned remedial actions to correct weaknesses or deficiencies and recommends agencies employ automated mechanisms to keep agency POA&Ms up to date, and readily available. OMB M-02-01 states that agencies' POA&Ms should identify, among other things, the origin of the finding, responsibilities for resolution, required funding and funding source, and milestones.[63] NIH policy aligns with NIST and further requires that all remedial actions be tracked in an agency-wide tool.

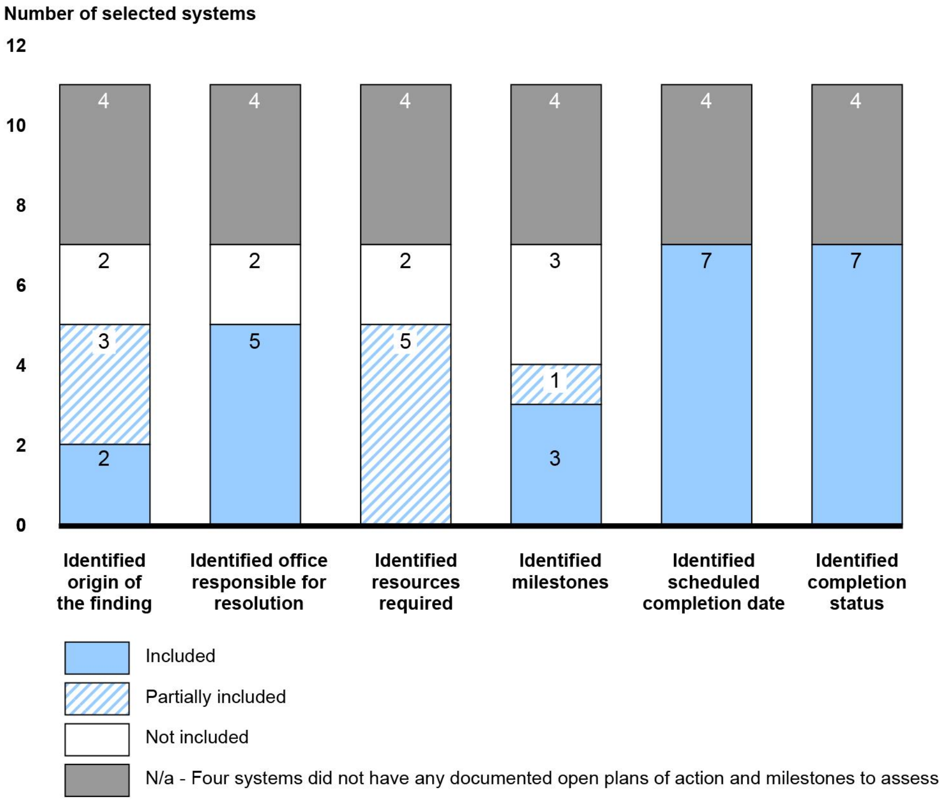
NIH took steps to develop procedures and processes to create, implement, and manage POA&Ms. NIH has also implemented an agency-wide tool for documenting and tracking these plans. However, three of the four selected entities did not always fully identify the origin of the finding, responsibilities for resolution, required resources, and milestones.[64]

[63] Office of Management and Budget, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, OMB M-02-01 (Washington, D.C.: Oct. 17, 2001).

[64] One entity did not have any open or recently closed plans of action and milestones (POA&Ms). As such, we were not able to assess the accuracy or completeness of the entity's remedial action activities or implementation of its POA&M tool.

Figure 4 provides an overview of NIH efforts to identify key elements for its information security remedial action review process.

Figure 4: GAO Assessment of U.S. National Institutes of Health (NIH) Selected Entities’ Implementation of Required Elements of Plans of Action and Milestones for Selected Systems



Source: GAO analysis of NIH data. | GAO-22-104467

Accessible Data Table for Figure 4

Number of selected systems	Included	Partially included	Not included	N/a – Four systems did not have any documented open plans of action milestones to asses
Identified origin of the finding	2	3	2	4
Identified office responsible for resolution	5	0	2	4
Identified resources required	0	5	2	4
Identified milestones	3	1	3	4
Identified scheduled completion date	7	0	0	4
Identified completion status	7	0	0	4

In addition, while officials at three entities tracked POA&Ms in NIH's agency-wide tracking tool, the fourth entity did not use the agency-wide tool to track these plans for one major system and 15 applications that operated on the system. For example, entity officials did not record 62 open POA&Ms associated with the 15 applications. Instead, the officials tracked these 62 plans in a separate entity-specific tool.[65]

Because the open POA&Ms were not tracked in the agency-wide tool, they were not subject to oversight from agency-wide officials. As a result, they were not included in deficiency reports sent by the ISAO team to entities nor were they included in the quarterly reports sent by the NIH CIO to the HHS CIO, although several of these applications were internet facing, contained sensitive information, and/or connected to the rest of the agency's network.

According to NIH officials, entities found the agency-wide tracking tool to be cumbersome, difficult to use, and lacking sufficient detail. Therefore, entities, such as the one cited in our example, developed their own tracking mechanisms to supplement the agency-wide tool. Nevertheless, the selected entities had not demonstrated that their documentation of POA&Ms was consistent with guidance.

[65] Entity officials had developed and maintained their own tool for tracking assessment and authorization data, including POA&Ms. This tool is not integrated with agency-wide tracking tools.

Until NIH and selected entities ensure that POA&Ms contain the required elements, the agency has an increased risk that it will not fully remediate deficiencies within established budgets and time frames. In addition, until all of the POA&Ms are tracked in the agency-wide tool, the ISAO team will be unable to provide oversight of the remediation process, provide accurate deficiency reports to entities, and will not possess critical information about existing vulnerabilities when considering whether to grant a system an authorization to operate.

NIH Did Not Always Update POA&Ms or Implement Remedial Actions in a Timely Manner

NIST SP 800-53 states that agencies should establish a frequency for updating POA&Ms based on findings from security assessments, analyses, and continuous monitoring activities. To ensure timely mitigation of program deficiencies, NIH developed a vulnerability remediation and POA&M policy that requires the plans be implemented by the scheduled completion date, documented within 30 days of a weakness being identified, and reviewed no less than quarterly.

NIH policy also defines time frames for remedial actions—high-risk deficiencies should be remediated within 60 days and moderate- and low-risk deficiencies should be remediated within 1 year. To ensure timely remediation and that past-due POA&Ms are addressed, the ISAO team provides regular deficiency reports to entities that highlight POA&Ms that had not been implemented.

However, three of the 11 selected systems had 16 POA&Ms with scheduled completion dates that were past due because the plans had not been updated at least quarterly or were incorrectly identified as not-implemented. For example, as of August 2019, 11 of the 16 that were past-due—three for one system and eight for another—had remedial actions implemented that were not reflected in the final disposition or milestones. NIH officials stated they were aware of the issue, and attributed it to the specific type of POA&Ms in question.[66] Subsequently, in March 2020, the agency stated that it had updated and closed nine of the 16 past-due plans as part of comprehensive updates and assessments conducted in 2019 and was in the process of remediating the remaining seven.

[66] According to entity officials responsible for these two systems, these types of POA&Ms could not be closed until they were verified by an external assessor.

Further, while officials at all four entities we reviewed had made efforts to remediate POA&Ms within the time frames required for selected systems, officials at one entity had not implemented 50 of the plans (13 of which were high risk). Specifically, as shown in table 4, entity officials had not remediated findings that had been open from 2 to 6 years as of December 2019.

Table 4: Plans of Action and Milestones Older Than 2 Years as of December 2019, by Assigned Risk, at One Selected Entity of the U.S. National Institutes of Health (NIH)

	Year in which the selected entity identified the deficiency				
Risk level	**2013**	**2014**	**2015**	**2016**	**2017**
High	1		11	1	
Medium	5	1	17	9	
Low	1		1	2	1

Source: GAO analysis of NIH data. | GAO-22-104467

According to NIH OCIO officials, they could only encourage entities to remediate POA&Ms. In addition, the officials said that they had not been aware of the one entity's open plans because that entity tracked the plans in a separate entity-specific tool instead of the agency-wide one. Until NIH updates and remediates POA&Ms, particularly those that are classified as high and medium risk, in a timely manner, NIH will have diminished situational awareness and security posture and its systems will be at increased risk that threats will exploit known and long-standing vulnerabilities.

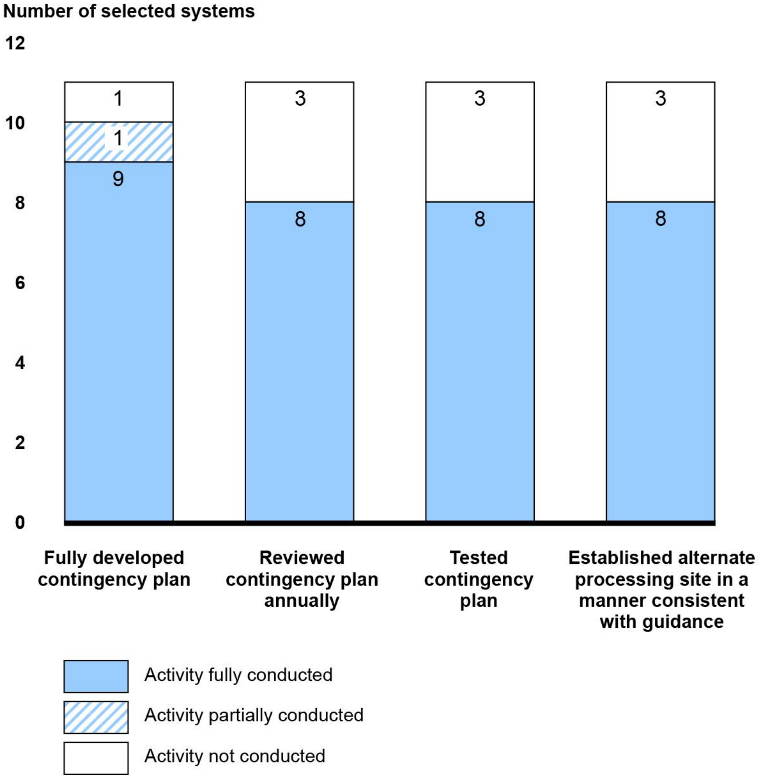
NIH Took Steps to Develop, Review, and Test Contingency Plans, but Improvements Are Needed for Some Systems

The *recover* core security function in the NIST cybersecurity framework is intended to support timely recovery of normal operations to reduce the impact from a cybersecurity event. Controls associated with this function include developing and testing contingency plans to ensure that, when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Losing the capability to process, retrieve, and protect information can significantly affect an agency's ability to accomplish its mission. If contingency planning is inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

FISMA requires plans and procedures to ensure continuity of operations for information systems. NIST SP 800-53 recommends that agencies develop, periodically review, and test a contingency plan for each system. NIST also recommends that agencies establish an alternate site for each moderate- and high-impact system and that the alternate site be separated from the primary site to reduce susceptibility to the same threats. NIH policy is consistent with NIST guidance, and requires entities to review and test systems' contingency plans annually.

NIH took steps to develop contingency plans for the majority of the selected systems, but did not fully develop two of the 11 contingency plans. For example, officials did not include all system locations for one system's contingency plan. In addition to plan development, while the agency took steps to review and test contingency plans, it did not do so for three of 11 systems. NIH also took steps to establish alternate processing sites, but did not establish sites for three of 11 selected systems in a manner consistent with guidance. Figure 5 below presents NIH's implementation of contingency plans for the selected systems.

Figure 5: GAO Assessment of U.S. National Institutes of Health (NIH) Selected Entities' Implementation of Contingency Planning Requirements for 11 Selected Information Systems



Source: GAO analysis of NIH data. | GAO-22-104467

Accessible Data Table for Figure 5

Number of selected systems	Activity fully conducted	Activity partially conducted	Activity not conducted
Fully developed contingency plan	9	1	1
Reviewed contingency plan annually	8	0	3
Tested contingency plan	8	0	3
Established alternate processing site in a manner consistent with guidance	8	0	3

OCIO officials stated that their contingency plans were generally complete, reviewed, and tested. Yet, the officials also noted that the selected entities were re-evaluating their systems' boundaries; thus, the entities had deferred updating and testing contingency plans, as well as establishing alternate processing sites, until the re-evaluation was complete. Entity officials did not have a documented time frame for completion of this effort.

In addition, in a written response, the agency stated that it did not have a process to ensure the quality of contingency plans. Agency officials further stated that each system's Business Impact Analysis documented the risk of not having an alternate processing site. While each system's Business Impact Analysis stated these systems did not meet the thresholds to justify the cost of an alternate processing site, no evidence was provided that stated what the threshold is, or that described a supporting rationale to back up the risk determination. Even without planning for an alternate processing site, the agency should have had plans in place to ensure it could restore essential mission functions in the event of a disruption.

Further, an entity CIO stated that the entity had not developed or tested a contingency plan for a key system because the system was covered by another system's documentation and testing. However, the other system's contingency plan documentation did not include the key system, or indicate that it was tested.

Until NIH takes additional steps to ensure that contingency plans are developed, tested, and annually reviewed for all information systems, the agency is at risk that it may not be able to recover mission essential functions, or ensure recovery activities are effective. Further, in not establishing and documenting alternate processing sites, NIH is at increased risk of disruption to mission essential functions.

NIH Has Fully Implemented about 28 Percent of Our Recommendations and Partially Implemented about 52 Percent

In our June 2021 report, we made 219 recommendations to NIH to strengthen its system controls and bolster its agency-wide information security program. Specifically, we recommended that the agency take 153 specific actions to resolve control deficiencies by implementing stronger access controls, encrypting sensitive data, configuring devices securely, applying patches in a timely manner, strengthening firewall rules, and implementing monitoring controls more effectively, among other things. We also made 66 recommendations for NIH to improve its information security program by, among other things, assessing risks as needed; documenting complete and accurate security controls; assessing controls more comprehensively; and remediating deficiencies in a timely manner. Table 5 shows the numbers of deficiencies and associated recommendations across the five core security functions.

Table 5: Number of Identified Control and Information Security Program Deficiencies at U.S. National Institutes of Health and Associated Recommendations by Core Security Function as of June 2021

Core security function	Number of selected system control deficiencies	Number of selected system control deficiency recommendations	Number of information security program deficiencies	Number of information security program recommendations
Identify	0	0	12	26
Protect	78	141	4	6
Detect	5	11	5	11
Respond	1	1	7	16
Recover	0	0	4	7
Total	**84**	**153**	**32**	**66**

Source: GAO. | GAO-22-104467

As of June 2021, NIH had taken action to address 80 percent of our recommendations, with 28 percent fully implemented and 52 percent partially implemented. Specifically, NIH has made progress in implementing the recommendations we made to resolve the system control deficiencies in the information systems we reviewed. As of June 2021, NIH had fully implemented 37 (about 24 percent) of the 153 recommendations we made to address deficiencies in the controls over the systems we reviewed. In addition, the agency had partially implemented 81 (about 53 percent) of the 153 recommendations. In these instances, NIH had made progress toward implementing the recommendations, but had not completed all of the necessary corrective actions for us to consider the recommendations fully implemented. For the remaining 35 recommendations, the agency had not yet provided sufficient evidence that it had taken actions to implement the recommendations.

Table 6 summarizes the status of NIH's efforts to implement the 153 recommendations that we made to resolve system control deficiencies in selected systems, as of June 2021, in the three core security functions where we identified deficiencies.

Table 6: Status of Efforts by U. S. National Institutes of Health (NIH) to Implement GAO's Recommendations for Selected System Control Deficiencies by Core Security Function, as of June 2021

Core security function	Number of selected system control deficiency recommendations	Status of system control deficiency recommendations		
		Implemented	Partially implemented	Not implemented
Identify	0	0	0	0
Protect	141	36	71	34
Detect	11	1	9	1

Respond	1	0	1	0
Recover	0	0	0	0
Totals	**153**	**37**	**81**	**35**

Legend:

Implemented—(NIH successfully completed actions to implement the recommendation)

Partially implemented—(NIH had made progress toward—but had not completed—implementing the recommendation)

Not implemented—(NIH had not provided sufficient evidence that it had taken action to implement the recommendation)

Source: GAO analysis of NIH data. | GAO-22-104467

By fully implementing 37 of these recommendations and partially implementing 81 more, NIH has reduced some risk within various control areas. Specifically, these efforts included areas such as protecting network boundaries, restricting privileged access and unauthorized disclosure, and preventing data compromise. These areas were highlighted in our June 2021 report as being particularly vulnerable.

NIH also made progress implementing recommendations we made to improve its information security program. With regard to the 66 recommendations related to its information security program, NIH had fully implemented 25 (about 38 percent) of the recommendations. In addition, the agency had partially implemented 33 (50 percent) of the 66 recommendations. Table 7 summarizes the status of NIH's efforts to implement these recommendations, which cover each of the five core security functions.

Table 7: Status of Efforts by U.S. National Institutes of Health (NIH) to Implement GAO's Recommendations for Improving its Information Security Program by Core Security Function, as of June 2021

Core security function	Number of selected system control deficiency recommendations	Status of system control deficiency recommendations		
		Implemented	Partially implemented	Not implemented
Identify	26	13	10	3
Protect	6	0	5	1
Detect	11	1	8	2
Respond	16	11	4	1
Recover	7	0	6	1
Totals	**66**	**25**	**33**	**8**

Legend:

Implemented—(NIH successfully completed actions to implement the recommendation)

Partially implemented—(NIH had made progress toward—but had not completed—implementing the recommendation)

Not implemented—(NIH had not provided sufficient evidence that it had taken action to implement the recommendation)

Source: GAO analysis of NIH data. | GAO-22-104467

By implementing 25 of these recommendations, NIH has improved the effectiveness of its information security program and further ensured the confidentiality, integrity, and availability of the information and information systems it operates. Specifically, the agency has implemented several recommendations to update department-wide policies and procedures, as well as to improve the quality of its documentation related to authorization of systems, including updating system security plans and risk assessments. In addition, NIH has taken steps to improve its capability to respond and recover by implementing recommendations to update and test incident response plans and better document and implement plans of actions and milestones.

NIH has also partially implemented an additional 33 recommendations. These recommendations included areas such as actions related to further protecting its environment by ensuring the annual review of privileged users' access, and ensuring personnel with access to information systems complete their required role-based and annual security awareness training. In addition, the agency has taken steps towards implementing recommendations related to conducting security control assessments, as well as updating and testing contingency plans.

Although NIH has made progress in implementing our recommendations, deficiencies remain. Fully implementing the open recommendations is essential to ensuring that the agency's systems and sensitive information are not at increased and unnecessary risk of unauthorized use, disclosure, modification, or disruption. We will continue to track NIH's implementation of our remaining recommendations that it had not fully implemented.

Agency Comments and Our Evaluation

HHS provided written comments on a draft of this report. In its comments, which are reprinted in appendix III, the department stated that the NIH Director and Principal Deputy Director, and the 27 Institute and Center Directors are united in their commitment to protect the confidentiality, integrity, and availability of NIH's data and information systems. HHS noted that NIH has reported implementing 53 of our 66 security program recommendations and 109 of our 153 system control deficiency recommendations. The department also stated that NIH expects to achieve closure on more than 93 percent of our recommendations within the next 6 months (June 2022), and to complete the implementation of all of our recommendations by December 2022. We will continue to follow-up with NIH to validate its implementation of recommendations beyond those cited in our report as fully implemented.

HHS stated that NIH had implemented many significant cybersecurity improvements and completed hundreds of actions to address our findings and recommendations. These actions included making complex architectural design and engineering changes to the agency’s network, as well as replacing thousands of outdated technology platforms that had reached the end of life and could no longer be adequately secured. The department highlighted several areas of improvement at NIH: assessing and managing risks; preventing unauthorized access and loss of data; securing systems and technologies; defending the network; monitoring, detecting, and responding to incidents; and incorporating cyber into everyday culture and work activities.

HHS also provided a technical comment, which we addressed in the report.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Health and Human Services, the HHS OCIO, and the department’s Inspector General, the Director of NIH, and interested congressional parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov. GAO staff who made key contributions to this report are listed in appendix IV.

Jennifer R. Franks
Director, Information Technology and Cybersecurity

Vijay A. D’Souza

Vijay A. D’Souza
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our first objective was to assess the extent to which NIH had effectively implemented an information security program and controls to protect the confidentiality, integrity, and availability of its information on selected information systems. In June 2021, we issued a report which detailed the findings from our work in response to this objective.[1] In the report, we made 153 recommendations to NIH to resolve the control deficiencies in the information systems we reviewed and 66 additional recommendations to improve its information security program. We designated that report as "limited official use only" (LOUO) and did not release it to the general public because of the sensitive information it contained.

This report publishes the findings discussed in our June 2021 report, but we have removed all references to the sensitive information. Specifically, we deleted the names of the information systems and computer networks that we examined, disassociated identified control deficiencies from named systems, deleted certain details about information security controls and control deficiencies, and omitted an appendix that was contained in the LOUO report. That appendix contained sensitive details about the control deficiencies in the NIH's information systems that we reviewed, and the 153 recommendations we made to mitigate those deficiencies. We also provided a draft of this report to NIH officials to review and comment on the sensitivity of the information contained herein and to affirm that the report can be made available to the public without jeopardizing the security of NIH's information systems and networks.

In addition, this report addresses a second objective that was not included in the June 2021 report. Specifically, this objective was to determine the extent to which NIH had taken corrective actions to address the previously identified security program and system control deficiencies and related recommendations for improvement that we identified in the earlier report.

As noted in our June 2021 report, we determined the extent to which NIH has effectively implemented information security controls to protect the

[1] GAO, *Cybersecurity: NIH Needs to Address Program and Control Deficiencies*, GAO-21-333SU (Washington, D.C.: June 30, 2021).

confidentiality, integrity, and availability of its information on selected information systems. To do this, we selected a risk-based, non-generalizable sample from the 123 reported information systems that NIH uses for biosafety labs, biomedical research, high performance computing, facilities maintenance, and administration. To do so, we focused on systems that: (1) collect, process, and maintain private or potentially sensitive proprietary business, personal medical health records, or personally identifiable information; (2) are essential to NIH's mission; (3) provide applications and controls for Biosafety Levels (BSL) 3 and 4 labs[2] that contain select agents,[3] which, if compromised, could pose a severe threat to public safety; and/or (4) share some common infrastructure.

We also took into consideration entities from among the agency's 28 institutes, centers, and the Office of the Director.[4] Our selection focused on entities that provide information technology and security for NIH and that are essential to the agency's mission.

Based on applying these criteria to systems and entities, we selected 11 mission-essential systems within four entities.[5] Of these systems, the agency had categorized five as high-impact systems, five as moderate-

[2] Biosafety levels (BSL) are used to identify the protective measures needed in a laboratory setting to protect workers, the environment, and the public. Research on agents not known to consistently cause disease in healthy adults is conducted in BSL-1 labs. Research on moderate-risk agents that pose a danger if accidentally inhaled, swallowed, or exposed to the skin is conducted in BSL-2 labs. Research on agents that can be transmitted through the air and cause potentially lethal infection is conducted in BSL-3 labs. Research on agents that pose a high risk of life-threatening disease for which no vaccine or therapy is available is conducted in BSL-4 labs.

[3] Select agents are biological agents and toxins that have the potential to pose a severe threat to public health and safety, to animal and plant health, or to animal or plant products.

[4] In this report, we use the term "entities" to represent NIH's institutes, centers, and office.

[5] We are not naming the four selected entities in this report due to the sensitive nature of the information.

impact systems, and one as a low-impact system.[6] The agency also considered one system to be a high-value asset that is of particular interest to potential adversaries.[7]

To evaluate NIH's information security controls—both for its information security program and selected systems—we based our assessment of controls on requirements identified by the *Federal Information Security Modernization Act of 2014* (FISMA),[8] which establishes key elements for an effective agency-wide information security program; National Institute of Standards and Technology (NIST) guidelines and standards;[9] HHS and NIH policies, procedures, and standards; and standards and guidelines from relevant security organizations, such as the National Security Agency, the Center for Internet Security,[10] and the Interagency Security

[6] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: February 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

[7] High-value assets refer to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical federal operations, or house unique collections of data (by size or content), making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. government.

[8] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[9] For example, see National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006), and National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

[10] The Center for Internet Security is a nonprofit entity that uses a global information technology community to safeguard private and public organizations against cyber threats. The Center also provides tools to assess implementation of industry best practices for information system security controls such as firewall rules and policy settings. We used a Center for Internet Security tool to assess NIH's information systems.

Committee.[11] In addition, to evaluate NIH's controls over its information systems, we used our *Federal Information System Controls Audit Manual,* which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.[12]

For reporting purposes, we categorized the security controls that we assessed into the five core security functions described in the NIST cybersecurity framework.[13] These five core security functions are identify, protect, detect, respond, and recover, which are discussed as follows:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[14]
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

For the *identify* core security function, we examined NIH's FISMA reports provided to the Office of Management and Budget and the Department of Homeland Security; reviewed the agency's information system inventory and reporting; analyzed impact categorizations and risk assessments for

[11] The Interagency Security Committee, an interagency organization chaired by the Department of Homeland Security, was established by Executive Order No. 12977, 60 Fed. Reg. 54411 (October 1995), to enhance the quality and effectiveness of security and the protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities. Executive Order No. 12977 was later amended by Executive Order No. 13286, 68 Fed. Reg. 10619 (March 2003). The organization is comprised of senior level executives from federal agencies and departments.

[12] GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009).

[13] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

[14] According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

the 11 selected systems to determine whether NIH identified threats, vulnerabilities, and impact from loss of confidentiality, integrity, or availability; examined authorization process documentation for consistency with guidance; analyzed NIH policies, procedures, and practices to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems; and analyzed security plans for the 11 selected systems to determine if those plans had been developed, documented, and updated according to federal guidance.

To evaluate the agency's development and reporting of its inventory of major information systems we reviewed, as noted above, NIH's FISMA reports and inventory. We also compared security plans against the agency's system inventory. In addition, we asked NIH to validate a list of potential major information systems not included in the inventory or FISMA reporting.

For our section regarding security plans, we analyzed a body of individual security controls. We established a set of 169 controls based on our areas of review. From those we selected a baseline of 65 controls, of which 58 constituted a random sample and seven constituted a judgmental sample.[15] However, based on system impact level, not all controls were applicable for the moderate- and low-impact systems.[16] We reviewed 54 controls for moderate systems and 29 for the low-impact system.

For the *protect* core security function, we examined access controls for the 11 systems. These controls included the complexity and expiration of password settings to determine if password management was being enforced; administrative users' system access permissions to determine whether their authorizations exceeded the access necessary to perform their assigned duties; firewall configurations, among other things, to determine whether system boundaries had been adequately protected;

[15] We selected a random sample from the target population of 169 key relevant controls. The controls in the target population were identified using professional judgment and relevance to the audit. We selected a judgmental sample to ensure a selection of controls critical to managing information security risks, such as those for system boundary protections, penetration testing, and intrusion detection.

[16] National Institute of Standards and Technology Special Publication 800-53 recommends that agencies implement additional controls to mitigate risks associated with the operation of higher impact systems. These controls may not be applicable for systems with lower impact ratings.

and physical security controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft.

In addition, we reviewed a random sample of privileged users to determine if selected agency entities had validated those users' access in a manner consistent with guidance. The sample was based on 404 privileged users missing from the records of privileged user access review that NIH submitted. We calculated that a sample of 198 privileged users would be sufficient to estimate the mean compliance rate of privileged user access reviews with a 5 percent margin of error for a 95 percent confidence interval. We added a further 15 samples in case records could not be found, which gave us a random sample of 213 records. We did not include the Office of the Director in the random sample because that office had only a small representation of privileged users for one of the selected systems.

We also examined configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted. In addition, we examined configuration settings for routers, network management servers, switches, firewalls, and workstations to determine if settings adhered to configuration standards, and inspected key servers and workstations to determine if critical patches had been installed and/or were up-to-date. Further, we examined training records to determine if employees and contractors had received security awareness training according to federal requirements, and whether personnel who have significant security responsibilities had received training commensurate with those responsibilities.

In order to demonstrate that users from selected entities met annual IT security awareness training requirements, we reviewed a random sample of employees with required IT training to determine if sampled individuals had a completed training record. The sample was based on 4,456 employees missing valid training records that NIH submitted. We calculated that a sample of 355 employees required to take annual awareness training would be sufficient to estimate the compliance rate of employees with a 5 percent margin of error for a 95 percent confidence interval. We added a further 15 samples to account for potentially duplicative records, which gave us a random sample of 370 records.

In addition, we reviewed a random sample of privileged users from selected entities required to take role-based training to determine if sampled individuals had a completed training record. The sample was based on 549 privileged users missing valid training records that NIH submitted. We calculated a sample of 227 privileged users required to take role-based training in order to estimate the compliance rate of employees with a 5 percent margin of error for a 95 percent confidence interval. We added a further 15 samples to account for potentially duplicative records, which gave us a random sample of 242 records.

For the *detect* core security function, we analyzed centralized logging and network traffic monitoring capabilities for key assets connected to the network; analyzed NIH's procedures and results for assessing security controls to determine whether controls for the 11 selected systems had been sufficiently tested at least annually and based on risk. We also reviewed the agency's implementation of continuous monitoring practices to determine whether the agency had developed and implemented a continuous monitoring strategy to manage its information technology assets and monitor the security configurations and vulnerabilities for those assets.

For our section regarding security assessments, we analyzed a body of individual security control assessments to determine if the agency sufficiently assessed controls. We established a set of 169 controls based on our areas of review. From those controls we selected a baseline of 65 controls, consisting of a random sample of 58 controls and seven constituted a judgmental sample.[17] However, based on system impact level, not all control assessments were applicable for the moderate- and low-impact systems. Accordingly, we reviewed 54 controls for moderate systems and 29 for the low-impact system.

For the *respond* core security function, we reviewed NIH's implementation of incident response plans and practices, including an examination of incident tickets for 10 incidents. The 10 incidents we evaluated were those the agency considered to be most significant over a 14 month period from January 2018 to February 2019. In addition, we examined the agency's process for implementing and documenting plans of corrective actions for the 11 selected mission-essential systems.

[17] We selected a random sample from the target population of 169 key relevant controls. The controls in the target population were identified using professional judgment and relevance to the audit. We selected a judgmental sample to ensure a selection of controls critical to managing information security risks, such as those for system boundary protections, penetration testing, and intrusion detection.

For the *recover* core security function, we examined contingency plans for 11 selected mission-essential systems to determine whether those plans had been developed and tested. In assessing NIH's controls associated with this function, as well as the other four core functions, we interviewed officials from the Office of the Chief Information Officer, as well as officials from the four selected entities, as needed.

Within the core security functions, as appropriate, we evaluated the elements of NIH's information security program based on elements required by FISMA. For example, we analyzed risk assessments, security plans, security control assessments, and remedial action plans for each of the 11 selected mission-essential systems. In addition, we assessed whether the agency had ensured staff had completed security awareness training and whether those with significant security responsibilities received commensurate training. We also evaluated NIH's security policies and procedures.

We supplemented our analyses with interviews of NIH personnel and observations of physical and environmental security controls. We conducted our reviews at agency facilities located in Bethesda and Frederick, Maryland; Hamilton, Montana; and Ashburn and Sterling, Virginia.

To determine the reliability of NIH's computer-processed data for information system inventories, user access, and training, we evaluated the materiality of the data to our audit objective and assessed the data by various means, including reviewing related documents, interviewing knowledgeable agency officials, and reviewing internal controls. Through these methods, we concluded that the data were sufficiently reliable for the purposes of our work, except for deficiencies noted in the report.

To accomplish our second objective—to determine the extent of NIH's actions to address the previously identified security program and system control deficiencies and related recommendations—we examined documentation provided by NIH. Specifically, for each recommendation that NIH indicated it had implemented as of June 4, 2021, we examined supporting documents to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve the underlying control deficiency. Based on this assessment, we categorized the status of each recommendation into one of three categories:

- **Implemented:** NIH successfully completed actions to implement the recommendation.

- **Partially implemented:** NIH had made progress toward—but had not completed—implementing the recommendation.
- **Not implemented:** NIH had not provided sufficient evidence that it has taken action to implement the recommendation.

We also determined that the control environment, risk assessment, control activities, information and communication, and monitoring components of internal control were significant to our objectives, along with numerous underlying principles. As previously described, we assessed these components by, among other things, evaluating risk assessments, information security program and system controls, and remediation activities.

We conducted this performance audit from January 2019 to December 2021 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: National Institute of Standards and Technology's Cybersecurity Framework

The National Institute of Standards and Technology's cybersecurity framework consists of five core functions: identify, protect, detect, respond, and recover.[1] Within the five functions are 23 categories and 108 subcategories (see table 8).

Table 8: National Institute of Standards and Technology Cybersecurity Framework

Category	Subcategory
Identify (ID) Function	
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.
	ID.AM-2: Software platforms and applications within the organization are inventoried.
	ID.AM-3: Organizational communication and data flows are mapped.
	ID.AM-4: External information systems are catalogued.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated.
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk,	ID.GV-1: Organizational cybersecurity policy is established and communicated.
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	ID.GV-4: Governance and risk management processes address cybersecurity risks.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented.
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.

Category	Subcategory
Identify (ID) Function	
	ID.RA-3: Threats, both internal and external, are identified and documented.
	ID.RA-4: Potential business impacts and likelihoods are identified.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
	ID.RA-6: Risk responses are identified and prioritized.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed.
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.
Protect (PR) Function	
Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
	PR.AC-2: Physical access to assets is managed and protected.
	PR.AC-3: Remote access is managed.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

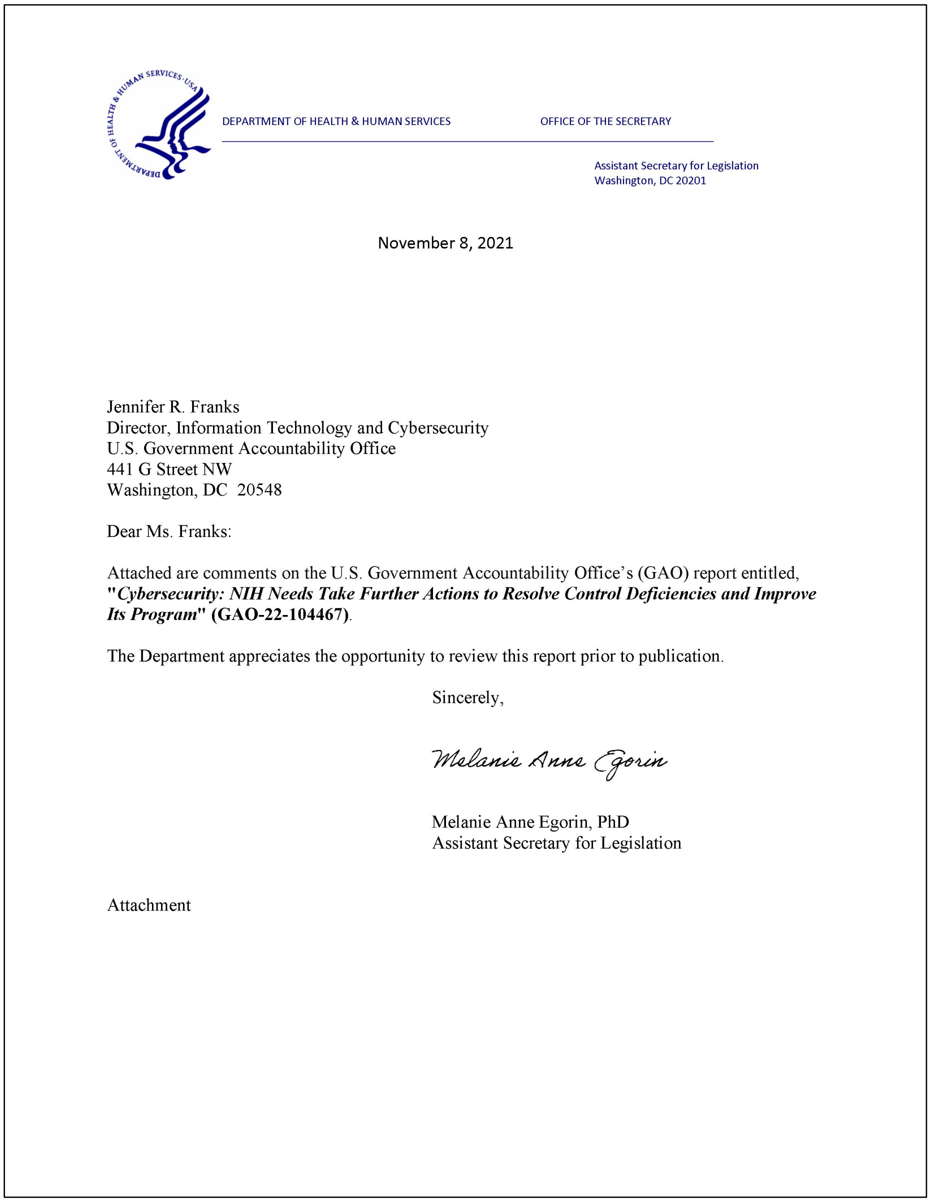
Category	Subcategory
Protect (PR) Function	
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained.
	PR.AT-2: Privileged users understand roles and responsibilities.
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles and responsibilities.
	PR.AT-4: Senior executives understand roles and responsibilities.
	PR.AT-5: Physical and cybersecurity personnel understand roles and responsibilities.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected.
	PR.DS-2: Data-in-transit is protected.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.
	PR.DS-4: Adequate capacity to ensure availability is maintained.
	PR.DS-5: Protections against data leaks are implemented.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
	PR.DS-7: The development and testing environment(s) are separate from the production environment.
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.
	PR.IP-3: Configuration change control processes are in place.
	PR.IP-4: Backups of information are conducted, maintained, and tested.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
	PR.IP-6: Data destroyed according to policy.
	PR.IP-7: Protection processes are improved.
	PR.IP-8: Effectiveness of protection technologies is shared.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	PR.IP-10: Response and recovery plans are tested.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

Category	Subcategory
Protect (PR) Function	
	PR.IP-12: A vulnerability management plan is developed and implemented.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets performed and logged, with approved and controlled tools.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
	PR.PT-2: Removable media is protected and its use restricted according to policy.
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
	PR.PT-4: Communications and control networks are protected.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
Detect (DE) Function	
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
	DE.AE-4: Impact of events is determined.
	DE.AE-5: Incident alert thresholds are established.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
	DE.CM-4: Malicious code is detected.
	DE.CM-5: Unauthorized mobile code is detected.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
	DE.CM-8: Vulnerability scans are performed.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.
	DE.DP-2: Detection activities comply with all applicable requirements.
	DE.DP-3: Detection processes are tested.
	DE.DP-4: Event detection information is communicated to parties.

Category	Subcategory
Detect (DE) Function	
	DE.DP-5: Detection processes are continuously improved.
Respond (RS) Function	
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed.
	RS.CO-2: Events are reported consistent with established criteria.
	RS.CO-3: Information is shared consistent with response plans.
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.
	RS.AN-2: The impact of the incident is understood.
	RS.AN-3: Forensics are performed.
	RS.AN-4: Incidents are categorized consistent with response plans.
	RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained.
	RS.MI-2: Incidents are mitigated.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.
Recover (RC) Function	
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incident.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.
	RC.IM-2: Recovery strategies are updated.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of attacking systems, victims, and vendors.	RC.CO-1: Public relations are managed.
	RC.CO-2: Reputation is repaired after an event.
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

Source: National Institute of Standards and Technology. | GAO-22-104467

Appendix III: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

November 8, 2021

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"*Cybersecurity: NIH Needs Take Further Actions to Resolve Control Deficiencies and Improve Its Program*" (GAO-22-104467)**.

The Department appreciates the opportunity to review this report prior to publication.

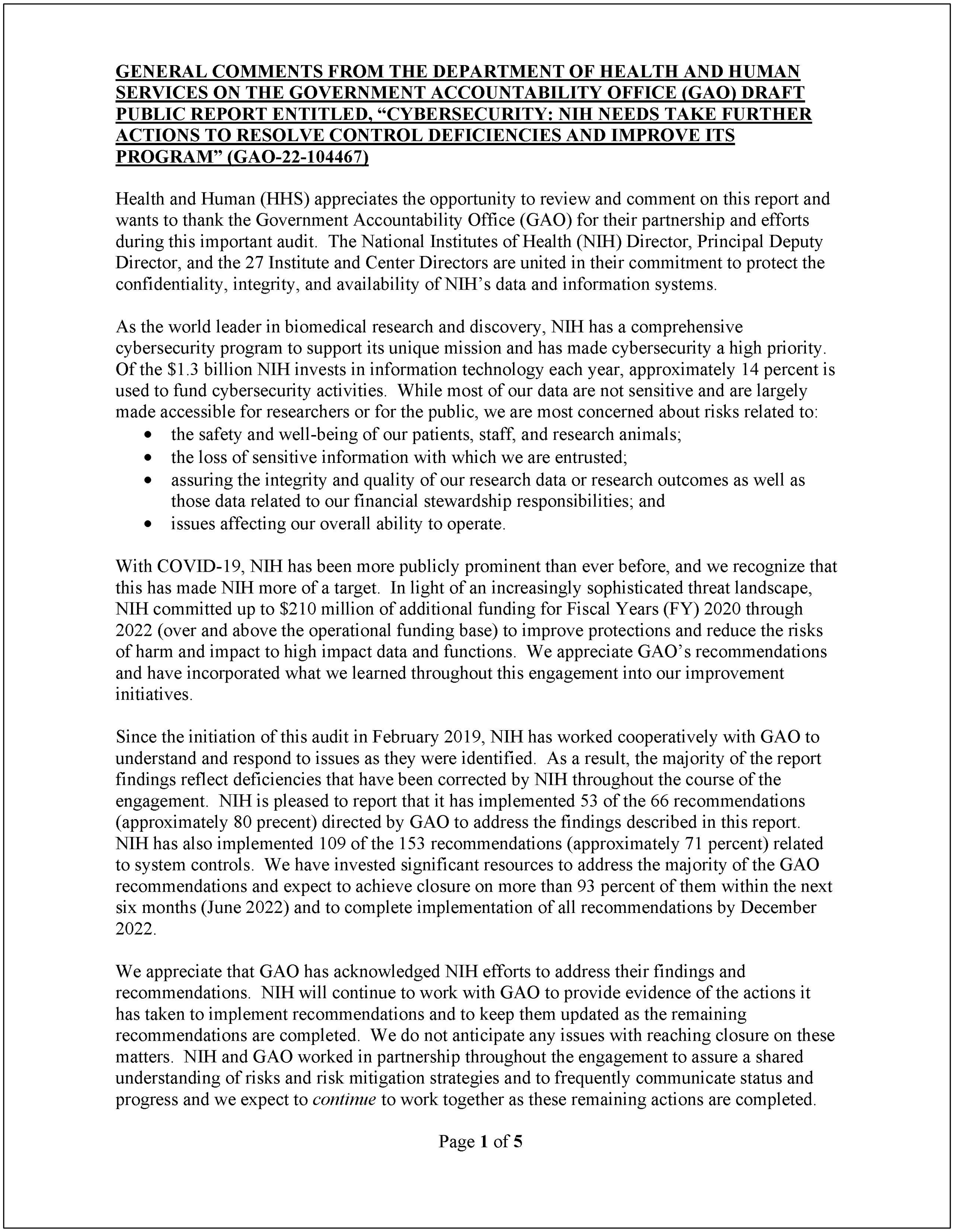
Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

Appendix III: Comments from the Department of Health and Human Services



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT PUBLIC REPORT ENTITLED, "CYBERSECURITY: NIH NEEDS TAKE FURTHER ACTIONS TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM" (GAO-22-104467)

Health and Human (HHS) appreciates the opportunity to review and comment on this report and wants to thank the Government Accountability Office (GAO) for their partnership and efforts during this important audit. The National Institutes of Health (NIH) Director, Principal Deputy Director, and the 27 Institute and Center Directors are united in their commitment to protect the confidentiality, integrity, and availability of NIH's data and information systems.

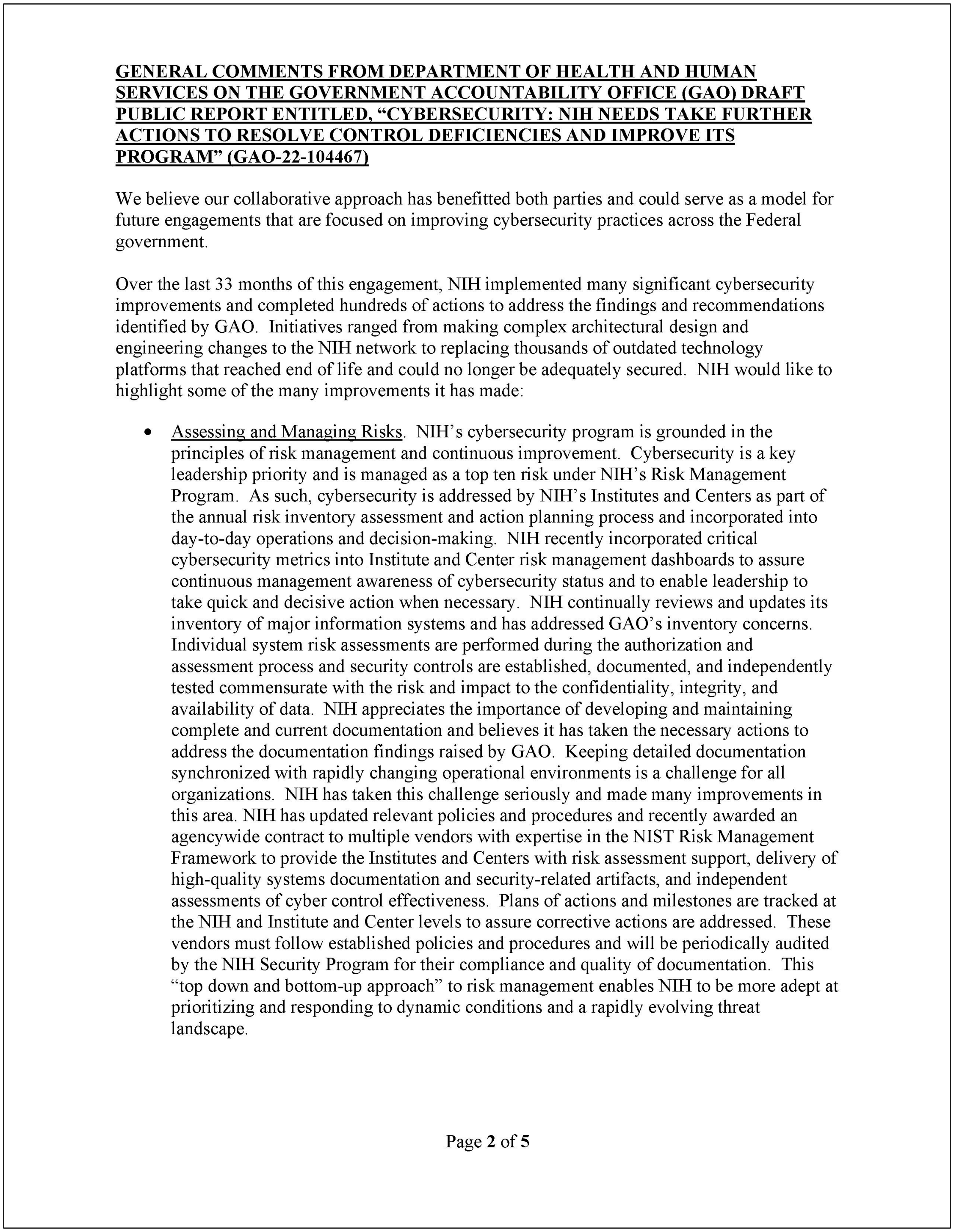
As the world leader in biomedical research and discovery, NIH has a comprehensive cybersecurity program to support its unique mission and has made cybersecurity a high priority. Of the $1.3 billion NIH invests in information technology each year, approximately 14 percent is used to fund cybersecurity activities. While most of our data are not sensitive and are largely made accessible for researchers or for the public, we are most concerned about risks related to:

- the safety and well-being of our patients, staff, and research animals;
- the loss of sensitive information with which we are entrusted;
- assuring the integrity and quality of our research data or research outcomes as well as those data related to our financial stewardship responsibilities; and
- issues affecting our overall ability to operate.

With COVID-19, NIH has been more publicly prominent than ever before, and we recognize that this has made NIH more of a target. In light of an increasingly sophisticated threat landscape, NIH committed up to $210 million of additional funding for Fiscal Years (FY) 2020 through 2022 (over and above the operational funding base) to improve protections and reduce the risks of harm and impact to high impact data and functions. We appreciate GAO's recommendations and have incorporated what we learned throughout this engagement into our improvement initiatives.

Since the initiation of this audit in February 2019, NIH has worked cooperatively with GAO to understand and respond to issues as they were identified. As a result, the majority of the report findings reflect deficiencies that have been corrected by NIH throughout the course of the engagement. NIH is pleased to report that it has implemented 53 of the 66 recommendations (approximately 80 precent) directed by GAO to address the findings described in this report. NIH has also implemented 109 of the 153 recommendations (approximately 71 percent) related to system controls. We have invested significant resources to address the majority of the GAO recommendations and expect to achieve closure on more than 93 percent of them within the next six months (June 2022) and to complete implementation of all recommendations by December 2022.

We appreciate that GAO has acknowledged NIH efforts to address their findings and recommendations. NIH will continue to work with GAO to provide evidence of the actions it has taken to implement recommendations and to keep them updated as the remaining recommendations are completed. We do not anticipate any issues with reaching closure on these matters. NIH and GAO worked in partnership throughout the engagement to assure a shared understanding of risks and risk mitigation strategies and to frequently communicate status and progress and we expect to *continue* to work together as these remaining actions are completed.

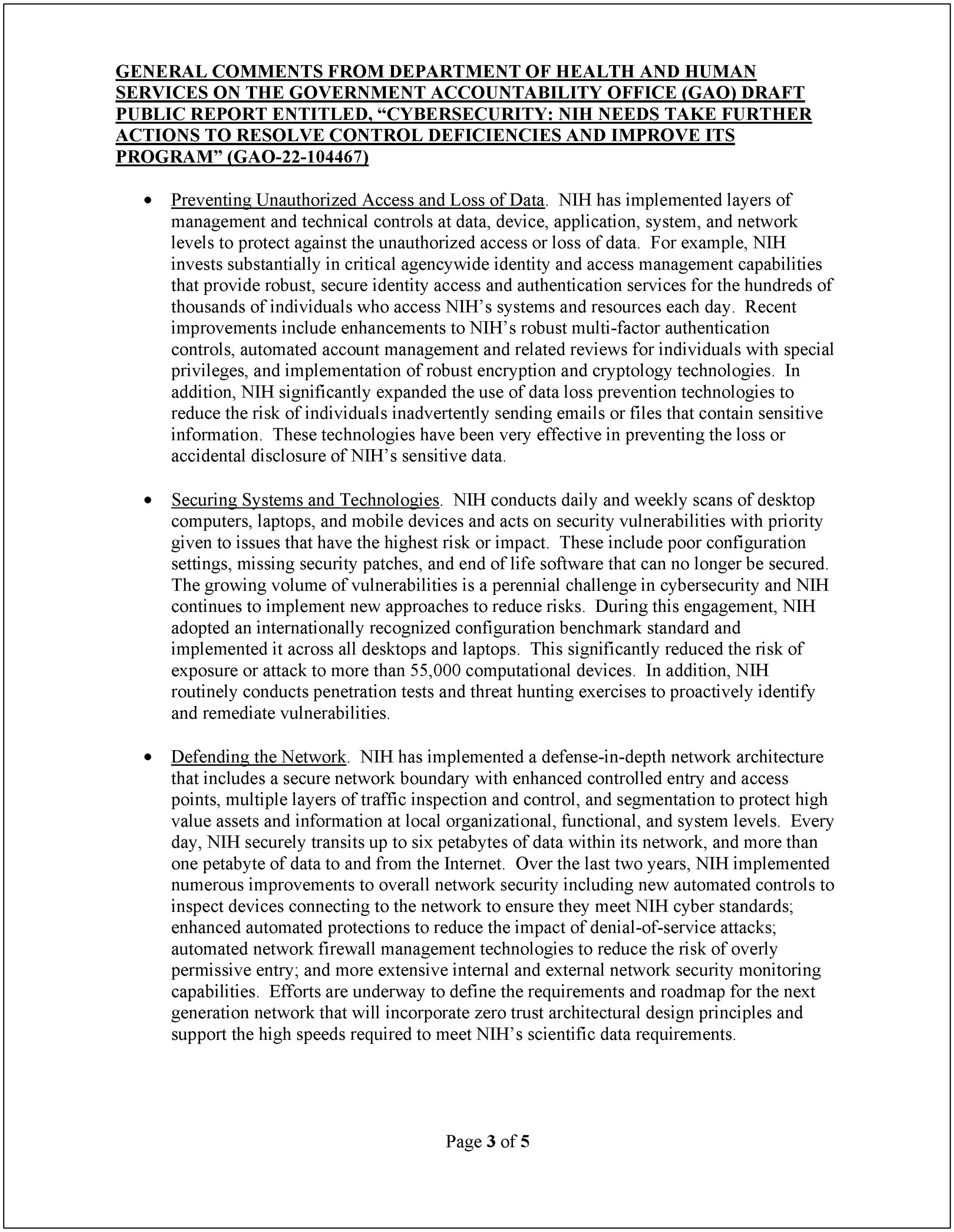


GENERAL COMMENTS FROM DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT PUBLIC REPORT ENTITLED, "CYBERSECURITY: NIH NEEDS TAKE FURTHER ACTIONS TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM" (GAO-22-104467)

We believe our collaborative approach has benefitted both parties and could serve as a model for future engagements that are focused on improving cybersecurity practices across the Federal government.

Over the last 33 months of this engagement, NIH implemented many significant cybersecurity improvements and completed hundreds of actions to address the findings and recommendations identified by GAO. Initiatives ranged from making complex architectural design and engineering changes to the NIH network to replacing thousands of outdated technology platforms that reached end of life and could no longer be adequately secured. NIH would like to highlight some of the many improvements it has made:

- Assessing and Managing Risks. NIH's cybersecurity program is grounded in the principles of risk management and continuous improvement. Cybersecurity is a key leadership priority and is managed as a top ten risk under NIH's Risk Management Program. As such, cybersecurity is addressed by NIH's Institutes and Centers as part of the annual risk inventory assessment and action planning process and incorporated into day-to-day operations and decision-making. NIH recently incorporated critical cybersecurity metrics into Institute and Center risk management dashboards to assure continuous management awareness of cybersecurity status and to enable leadership to take quick and decisive action when necessary. NIH continually reviews and updates its inventory of major information systems and has addressed GAO's inventory concerns. Individual system risk assessments are performed during the authorization and assessment process and security controls are established, documented, and independently tested commensurate with the risk and impact to the confidentiality, integrity, and availability of data. NIH appreciates the importance of developing and maintaining complete and current documentation and believes it has taken the necessary actions to address the documentation findings raised by GAO. Keeping detailed documentation synchronized with rapidly changing operational environments is a challenge for all organizations. NIH has taken this challenge seriously and made many improvements in this area. NIH has updated relevant policies and procedures and recently awarded an agencywide contract to multiple vendors with expertise in the NIST Risk Management Framework to provide the Institutes and Centers with risk assessment support, delivery of high-quality systems documentation and security-related artifacts, and independent assessments of cyber control effectiveness. Plans of actions and milestones are tracked at the NIH and Institute and Center levels to assure corrective actions are addressed. These vendors must follow established policies and procedures and will be periodically audited by the NIH Security Program for their compliance and quality of documentation. This "top down and bottom-up approach" to risk management enables NIH to be more adept at prioritizing and responding to dynamic conditions and a rapidly evolving threat landscape.

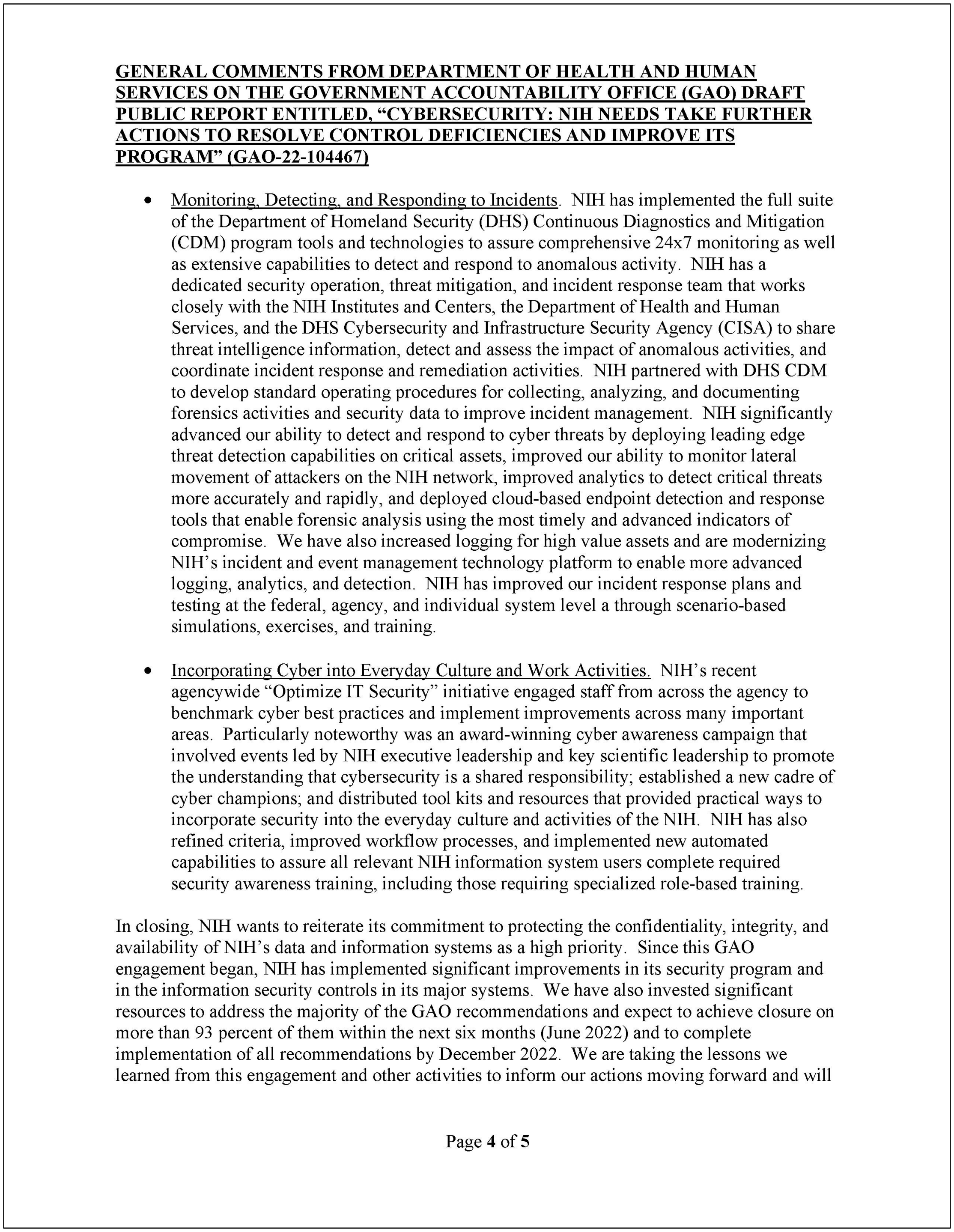


GENERAL COMMENTS FROM DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT PUBLIC REPORT ENTITLED, "CYBERSECURITY: NIH NEEDS TAKE FURTHER ACTIONS TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM" (GAO-22-104467)

- Preventing Unauthorized Access and Loss of Data. NIH has implemented layers of management and technical controls at data, device, application, system, and network levels to protect against the unauthorized access or loss of data. For example, NIH invests substantially in critical agencywide identity and access management capabilities that provide robust, secure identity access and authentication services for the hundreds of thousands of individuals who access NIH's systems and resources each day. Recent improvements include enhancements to NIH's robust multi-factor authentication controls, automated account management and related reviews for individuals with special privileges, and implementation of robust encryption and cryptology technologies. In addition, NIH significantly expanded the use of data loss prevention technologies to reduce the risk of individuals inadvertently sending emails or files that contain sensitive information. These technologies have been very effective in preventing the loss or accidental disclosure of NIH's sensitive data.

- Securing Systems and Technologies. NIH conducts daily and weekly scans of desktop computers, laptops, and mobile devices and acts on security vulnerabilities with priority given to issues that have the highest risk or impact. These include poor configuration settings, missing security patches, and end of life software that can no longer be secured. The growing volume of vulnerabilities is a perennial challenge in cybersecurity and NIH continues to implement new approaches to reduce risks. During this engagement, NIH adopted an internationally recognized configuration benchmark standard and implemented it across all desktops and laptops. This significantly reduced the risk of exposure or attack to more than 55,000 computational devices. In addition, NIH routinely conducts penetration tests and threat hunting exercises to proactively identify and remediate vulnerabilities.

- Defending the Network. NIH has implemented a defense-in-depth network architecture that includes a secure network boundary with enhanced controlled entry and access points, multiple layers of traffic inspection and control, and segmentation to protect high value assets and information at local organizational, functional, and system levels. Every day, NIH securely transits up to six petabytes of data within its network, and more than one petabyte of data to and from the Internet. Over the last two years, NIH implemented numerous improvements to overall network security including new automated controls to inspect devices connecting to the network to ensure they meet NIH cyber standards; enhanced automated protections to reduce the impact of denial-of-service attacks; automated network firewall management technologies to reduce the risk of overly permissive entry; and more extensive internal and external network security monitoring capabilities. Efforts are underway to define the requirements and roadmap for the next generation network that will incorporate zero trust architectural design principles and support the high speeds required to meet NIH's scientific data requirements.

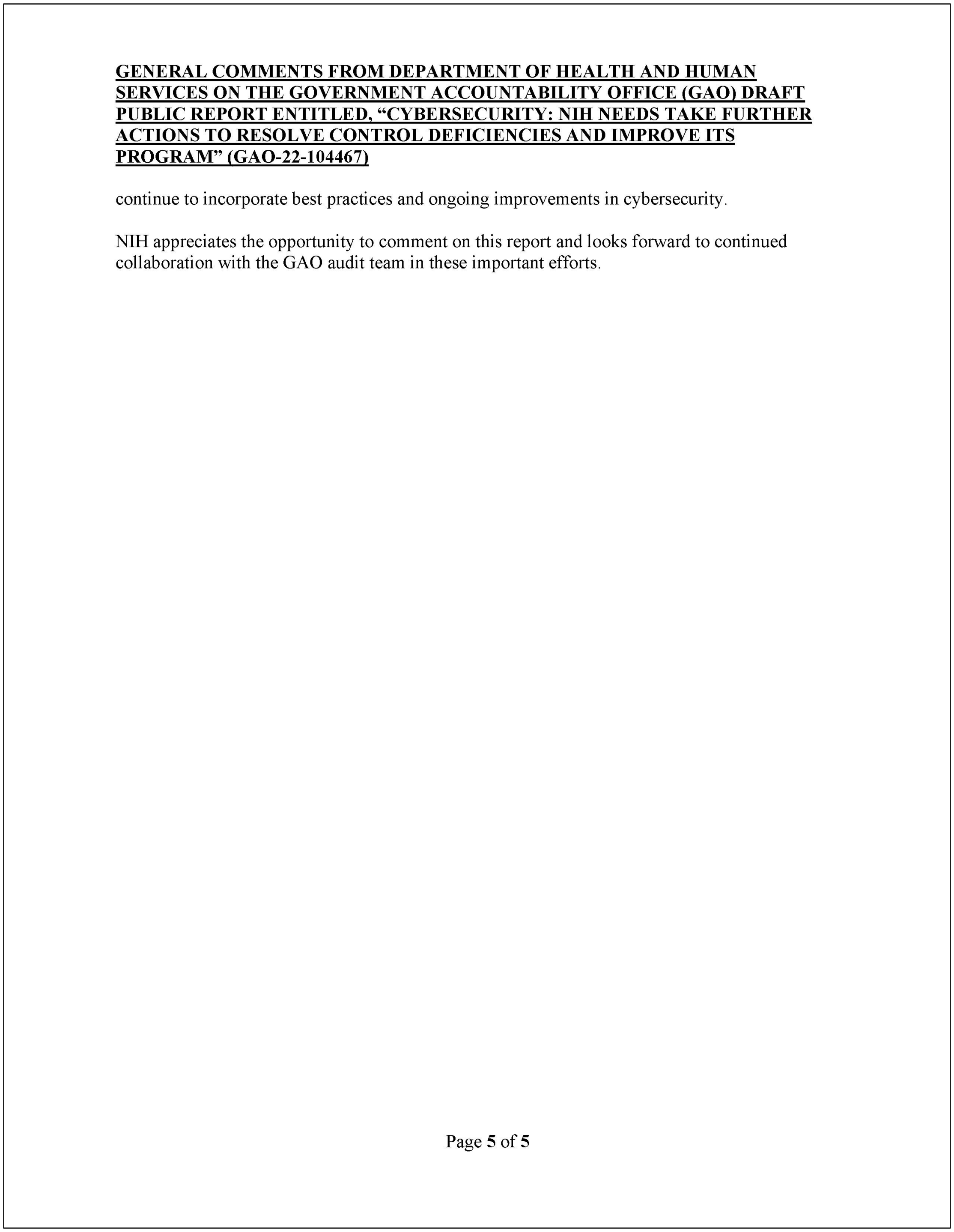


GENERAL COMMENTS FROM DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT PUBLIC REPORT ENTITLED, "CYBERSECURITY: NIH NEEDS TAKE FURTHER ACTIONS TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM" (GAO-22-104467)

- Monitoring, Detecting, and Responding to Incidents. NIH has implemented the full suite of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program tools and technologies to assure comprehensive 24x7 monitoring as well as extensive capabilities to detect and respond to anomalous activity. NIH has a dedicated security operation, threat mitigation, and incident response team that works closely with the NIH Institutes and Centers, the Department of Health and Human Services, and the DHS Cybersecurity and Infrastructure Security Agency (CISA) to share threat intelligence information, detect and assess the impact of anomalous activities, and coordinate incident response and remediation activities. NIH partnered with DHS CDM to develop standard operating procedures for collecting, analyzing, and documenting forensics activities and security data to improve incident management. NIH significantly advanced our ability to detect and respond to cyber threats by deploying leading edge threat detection capabilities on critical assets, improved our ability to monitor lateral movement of attackers on the NIH network, improved analytics to detect critical threats more accurately and rapidly, and deployed cloud-based endpoint detection and response tools that enable forensic analysis using the most timely and advanced indicators of compromise. We have also increased logging for high value assets and are modernizing NIH's incident and event management technology platform to enable more advanced logging, analytics, and detection. NIH has improved our incident response plans and testing at the federal, agency, and individual system level a through scenario-based simulations, exercises, and training.

- Incorporating Cyber into Everyday Culture and Work Activities. NIH's recent agencywide "Optimize IT Security" initiative engaged staff from across the agency to benchmark cyber best practices and implement improvements across many important areas. Particularly noteworthy was an award-winning cyber awareness campaign that involved events led by NIH executive leadership and key scientific leadership to promote the understanding that cybersecurity is a shared responsibility; established a new cadre of cyber champions; and distributed tool kits and resources that provided practical ways to incorporate security into the everyday culture and activities of the NIH. NIH has also refined criteria, improved workflow processes, and implemented new automated capabilities to assure all relevant NIH information system users complete required security awareness training, including those requiring specialized role-based training.

In closing, NIH wants to reiterate its commitment to protecting the confidentiality, integrity, and availability of NIH's data and information systems as a high priority. Since this GAO engagement began, NIH has implemented significant improvements in its security program and in the information security controls in its major systems. We have also invested significant resources to address the majority of the GAO recommendations and expect to achieve closure on more than 93 percent of them within the next six months (June 2022) and to complete implementation of all recommendations by December 2022. We are taking the lessons we learned from this engagement and other activities to inform our actions moving forward and will



continue to incorporate best practices and ongoing improvements in cybersecurity.

NIH appreciates the opportunity to comment on this report and looks forward to continued collaboration with the GAO audit team in these important efforts.

Agency Comment Letter

Text of Appendix III: Comments from the Department of Health and Human Services

Page 1

November 8, 2021

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"*Cybersecurity: NIH Needs Take Further Actions to Resolve Control Deficiencies and Improve Its Program*" (GAO-22-104467)**.

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin,PhD
Assistant Secretary for Legislation

Attachment

Page 2

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT PUBLIC REPORT ENTITLED, "CYBERSECURITY: NIH NEEDS TAKE FURTHER ACTIONS TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM" (GAO-22-104467)

Health and Human (HHS) appreciates the opportunity to review and comment on this report and wants to thank the Government Accountability Office (GAO) for their partnership and efforts during this important audit. The National Institutes of Health (NIH) Director, Principal Deputy Director, and the 27 Institute and Center Directors are united in their commitment to protect the confidentiality, integrity, and availability of NIH's data and information systems.

As the world leader in biomedical research and discovery, NIH has a comprehensive cybersecurity program to support its unique mission and has made cybersecurity a high priority. Of the $1.3 billion NIH invests in information technology each year, approximately 14 percent is used to fund cybersecurity activities. While most of our data are not sensitive and are largely made accessible for researchers or for the public, we are most concerned about risks related to:

- the safety and well-being of our patients, staff, and research animals;
- the loss of sensitive information with which we are entrusted;
- assuring the integrity and quality of our research data or research outcomes as well as those data related to our financial stewardship responsibilities; and
- issues affecting our overall ability to operate.

With COVID-19, NIH has been more publicly prominent than ever before, and we recognize that this has made NIH more of a target. In light of an increasingly sophisticated threat landscape, NIH committed up to $210 million of additional funding for Fiscal Years (FY) 2020 through 2022 (over and above the operational funding base) to improve protections and reduce the risks of harm and impact to high impact data and functions. We appreciate GAO's recommendations and have incorporated what we learned throughout this engagement into our improvement initiatives.

Since the initiation of this audit in February 2019, NIH has worked cooperatively with GAO to understand and respond to issues as they were identified. As a result, the majority of the report findings reflect deficiencies that have been corrected by NIH throughout the course of the engagement. NIH is pleased to report that it has implemented 53 of the 66 recommendations (approximately 80 precent) directed by GAO to address the findings described in this report.

NIH has also implemented 109 of the 153 recommendations (approximately 71 percent) related to system controls. We have invested significant resources to address the majority of the GAO recommendations and expect to achieve closure on more than 93 percent of them within the next six months (June 2022) and to complete implementation of all recommendations by December 2022.

We appreciate that GAO has acknowledged NIH efforts to address their findings and recommendations. NIH will continue to work with GAO to provide evidence of the actions it has taken to implement recommendations and to keep them updated as the remaining recommendations are completed. We do not anticipate any issues with reaching closure on these matters. NIH and GAO worked in partnership throughout the engagement to assure a shared understanding of risks and risk mitigation strategies and to frequently communicate status and progress and we expect to *continue* to work together as these remaining actions are completed.

Page 3

We believe our collaborative approach has benefitted both parties and could serve as a model for future engagements that are focused on improving cybersecurity practices across the Federal government.

Over the last 33 months of this engagement, NIH implemented many significant cybersecurity improvements and completed hundreds of actions to address the findings and recommendations identified by GAO. Initiatives ranged from making complex architectural design and engineering changes to the NIH network to replacing thousands of outdated technology platforms that reached end of life and could no longer be adequately secured. NIH would like to highlight some of the many improvements it has made:

Assessing and Managing Risks. NIH's cybersecurity program is grounded in the principles of risk management and continuous improvement. Cybersecurity is a key leadership priority and is managed as a top ten risk under NIH's Risk Management Program. As such, cybersecurity is addressed by NIH's Institutes and Centers as part of the annual risk inventory assessment and action planning process and incorporated into day-to-day operations and decision-making. NIH recently incorporated critical cybersecurity metrics into Institute and Center risk management dashboards to assure continuous management awareness of cybersecurity status and to enable leadership to take quick and decisive action when necessary. NIH continually reviews and updates its inventory of major information systems and has addressed GAO's inventory concerns. Individual system risk assessments are performed during the authorization and assessment process and security controls are established, documented, and independently tested commensurate with the risk and impact to the confidentiality, integrity, and availability of data. NIH appreciates the importance of developing and maintaining complete and current documentation and believes it has taken the necessary actions to address the documentation findings raised by GAO. Keeping detailed documentation synchronized with rapidly changing operational environments is a challenge for all organizations. NIH has taken this challenge seriously and made many improvements in this area. NIH has updated relevant policies and procedures and recently awarded an agencywide contract to multiple vendors with expertise in the NIST Risk Management Framework to provide the Institutes and Centers with risk assessment support, delivery of high-quality systems documentation and security-related artifacts, and independent assessments of cyber control effectiveness. Plans of actions and milestones are tracked at the NIH and Institute and Center levels to assure corrective actions are addressed. These vendors must follow established policies and procedures and will be periodically audited by the NIH Security Program for their compliance and quality of documentation. This "top down and bottom-up approach" to risk management enables NIH to be more adept at prioritizing and responding to dynamic conditions and a rapidly evolving threat landscape.

Page 4

- Preventing Unauthorized Access and Loss of Data. NIH has implemented layers of management and technical controls at data, device, application, system, and network levels to protect against the unauthorized access or loss of data. For example, NIH invests substantially in critical agencywide identity and access management capabilities that provide robust, secure identity access and authentication services for the hundreds of thousands of individuals who access NIH's systems and resources each day. Recent improvements include enhancements to NIH's robust multi-factor authentication controls, automated account management and related reviews for individuals with special privileges, and implementation of robust encryption and cryptology technologies. In addition, NIH significantly expanded the use of data loss prevention technologies to reduce the risk of individuals inadvertently sending emails or files that contain sensitive information. These technologies have been very effective in preventing the loss or accidental disclosure of NIH's sensitive data.

- Securing Systems and Technologies. NIH conducts daily and weekly scans of desktop computers, laptops, and mobile devices and acts on security vulnerabilities with priority given to issues that have the highest risk or impact. These include poor configuration settings, missing security patches, and end of life software that can no longer be secured. The growing volume of vulnerabilities is a perennial challenge in cybersecurity and NIH continues to implement new approaches to reduce risks. During this engagement, NIH adopted an internationally recognized configuration benchmark standard and implemented it across all desktops and laptops. This significantly reduced the risk of exposure or attack to more than 55,000 computational devices. In addition, NIH routinely conducts penetration tests and threat hunting exercises to proactively identify and remediate vulnerabilities.

Defending the Network. NIH has implemented a defense-in-depth network architecture that includes a secure network boundary with enhanced controlled entry and access points, multiple layers of traffic inspection and control, and segmentation to protect high value assets and information at local organizational, functional, and system levels. Every day, NIH securely transits up to six petabytes of data within its network, and more than one petabyte of data to and from the Internet. Over the last two years, NIH implemented numerous improvements to overall network security including new automated controls to inspect devices connecting to the network to ensure they meet NIH cyber standards; enhanced automated protections to reduce the impact of denial-of-service attacks; automated network firewall management technologies to reduce the risk of overly permissive entry; and more extensive internal and external network security monitoring capabilities. Efforts are underway to define the requirements and roadmap for the next generation network that will incorporate zero trust architectural design principles and support the high speeds required to meet NIH's scientific data requirements.

Page 5

- Monitoring, Detecting, and Responding to Incidents. NIH has implemented the full suite of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program tools and technologies to assure comprehensive 24x7 monitoring as well as extensive capabilities to detect and respond to anomalous activity. NIH has a dedicated security operation, threat mitigation, and incident response team that works closely with the NIH Institutes and Centers, the Department of Health and Human Services, and the DHS Cybersecurity and Infrastructure Security Agency (CISA) to share threat intelligence information, detect and assess the impact of anomalous activities, and coordinate incident response and remediation activities. NIH partnered with DHS CDM to develop standard operating procedures for collecting, analyzing, and documenting forensics activities and security data to improve incident management. NIH significantly advanced our ability to detect and respond to cyber threats by deploying leading edge threat detection capabilities on critical assets, improved our ability to monitor lateral movement of attackers on the NIH network, improved analytics to detect critical threats more accurately and rapidly, and deployed cloud-based endpoint detection and response tools that enable forensic analysis using the most timely and advanced indicators of compromise. We have also increased logging for high value assets and are modernizing NIH's incident and event management technology platform to enable more advanced logging, analytics, and detection. NIH has improved our incident response plans and testing at the federal, agency, and individual system level a through scenario-based simulations, exercises, and training.

- Incorporating Cyber into Everyday Culture and Work Activities. NIH's recent agencywide "Optimize IT Security" initiative engaged staff from across the agency to benchmark cyber best practices and implement improvements across many important areas. Particularly noteworthy was an award-winning cyber awareness campaign that involved events led by NIH executive leadership and key scientific leadership to promote the understanding that cybersecurity is a shared responsibility; established a new cadre of cyber champions; and distributed tool kits and resources that provided practical ways to incorporate security into the everyday culture and activities of the NIH. NIH has also refined criteria, improved workflow processes, and implemented new automated capabilities to assure all relevant NIH information system users complete required security awareness training, including those requiring specialized role-based training.

In closing, NIH wants to reiterate its commitment to protecting the confidentiality, integrity, and availability of NIH's data and information systems as a high priority. Since this GAO engagement began, NIH has implemented significant improvements in its security program and in the information security controls in its major systems. We have also invested significant resources to address the majority of the GAO recommendations and expect to achieve closure on more than 93 percent of them within the next six months (June 2022) and to complete implementation of all recommendations by December 2022. We are taking the lessons we learned from this engagement and other activities to inform our actions moving forward and will

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Gary Austin, West Coile, Saar Dagani, Jeffrey Knott, Harold Lewis, and Chris Warweg (assistant directors); Alexander Anderegg and Brandon Sanders (analysts-in-charge); Logan Arkema, John Bailey, Angela Bell, Vijay A. D'Souza, Ahmad Ferguson, Charles Hubbard III, Carlton Maynard, Sean Mays, Tarunkant Mithani, Julia Munroe, Monica Perez-Nelson, Priscilla Smith, Daniel Spence, Michael Stevens, Khristi Wilkins, and Gregory C. Wilshusen made key contributions to this report. Christopher Businsky, Corey Evans, Nancy Glover, Teea Kim, Sailaja Ledalla, Duc Ngo, Freda Paintsil, Brandon S. Pettis, Zsaroq Powe, and Daniel Swartz also provided assistance.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548