United States Government Accountability Office

Report to Congressional Requesters

December 2018

INFORMATION SECURITY

Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program

Accessible Version

GAO-19-70

GAO Highlights

Highlights of GAO-19-70, a report to congressional requesters

December 2018

INFORMATION SECURITY

Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program

Why GAO Did This Study

CDC is responsible for detecting and responding to emerging health threats and controlling dangerous substances. In carrying out its mission, CDC relies on information technology systems to receive, process, and maintain sensitive data. Accordingly, effective information security controls are essential to ensure that the agency's systems and information are protected from misuse and modification.

GAO was asked to examine information security at CDC. In June 2018, GAO issued a limited official use only report on the extent to which CDC had effectively implemented technical 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 2018 report. In addition, for this public report, GAO determined the extent to which CDC has taken corrective actions to address the previously identified security program and technical control deficiencies and related recommendations for improvement. For this report, GAO reviewed supporting documents regarding CDC's actions on previously identified recommendations and interviewed personnel at CDC.

View GAO-19-70. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

As GAO reported in June 2018, the Centers for Disease Control and Prevention (CDC) implemented technical controls and an information security program that were intended to safeguard the confidentiality, integrity, and availability of its information systems and information. However, GAO identified 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 below). GAO made 195 recommendations to address these deficiencies.

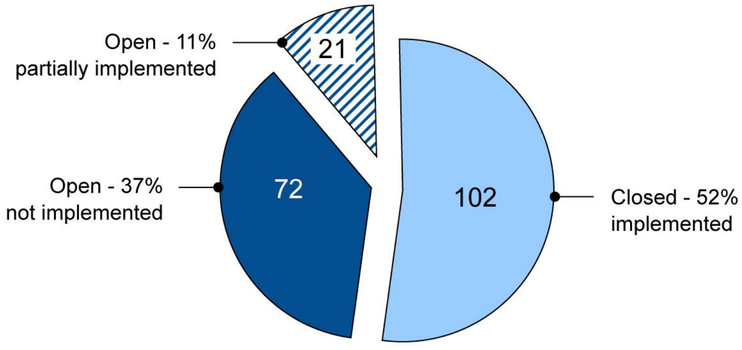
Number of GAO-Identified Technical Control and Information Security Program Deficiencies at the Centers for Disease Control and Prevention and Associated Recommendations by Core Security Function

Core security function	Number of technical control deficiencies	Number of technical control recommendations	Number of information security program deficiencies	Number of information security program recommendations
Identify	0	0	5	5
Protect	85	161	1	1
Detect	8	18	3	3
Respond	1	5	1	1
Recover	0	0	1	1
Total	**94**	**184**	**11**	**11**

Source: GAO. | GAO-19-70

As of August 2018, CDC had made significant progress in resolving many of the security deficiencies by implementing 102 of 184 (about 55 percent) technical control recommendations, and partially implementing 1 of 11 information security program recommendations made in the June 2018 report. The figure shows the status of CDC's efforts to implement the 195 recommendations.

Status of GAO Recommendations to the Centers for Disease Control and Prevention



Source: GAO analysis of CDC data. | GAO-19-70

Additionally, CDC has created remedial action plans to implement the majority of the remaining open recommendations by September 2019. Until CDC 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

Tables

Figures

Abbreviations

CDM	continuous diagnostics and mitigation
CIO	chief information officer
CISO	chief information security officer
CDC	Centers for Disease Control and Prevention
DMZ	demilitarized zone
ISCM	information security continuous monitoring
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
HHS	Department of Health and Human Services
ISC	Interagency Security Committee
ISSO	information systems security officer
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
PIV	personal identity verification
POA&M	plan of actions and milestones
SP	special publication

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

December 20, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Trey Gowdy
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Fred Upton
House of Representatives

The Centers for Disease Control and Prevention (CDC) is responsible for protecting America from both foreign and domestic health, safety, and security threats. Its roles include detecting and responding to new and emerging health threats, tackling the biggest health problems causing death and disability for Americans, putting science and advanced technology into action to prevent disease, and controlling dangerous and exotic substances that can cause incurable and deadly diseases. Performing these roles may involve tracking diseases and finding out what is making people sick and the most effective ways to prevent diseases.

CDC confronts global disease threats through advanced computing and laboratory analysis of large amounts of data to find solutions, making use of computer systems critical to the process. However, cyber incidents at federal agencies demonstrate the damage that increasingly sophisticated threats can cause and underscore the importance of effectively protecting federal systems, including those used by CDC to achieve its mission.

Since 1997, we have designated the security of information on 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 CDC performs and concerns over the security of federal information systems, you requested that we examine the security controls over key CDC systems. Accordingly, our specific objective was to assess the extent to which CDC 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 2018, we issued a report that addressed the extent to which CDC 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 184 recommendations to CDC to resolve the technical security control deficiencies in the information systems we reviewed and 11 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 subsequent report publishes the findings discussed in our June 2018 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. The appendix contained sensitive details about the technical security control deficiencies in CDC's information systems and computer networks that we reviewed, and the 184 recommendations we made to mitigate those deficiencies. We also provided a draft of this report to CDC 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 CDC's information systems and networks.

[1] For our latest high-risk report, see GAO*, High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[2] GAO, *Information Security: CDC Needs to Improve Its Program and Resolve Control Deficiencies*, GAO-18-437SU (Washington, D.C.: June 20, 2018).

In addition, this report addresses a second objective that was not included in the June 2018 report. Specifically, this objective was to determine the extent to which CDC has taken corrective actions to address the previously identified security program and technical control deficiencies and related recommendations for improvement that we identified in the earlier report.

As noted in our LOUO report, to accomplish the first objective—to determine the extent to which CDC had effectively implemented an information security program and controls—we had examined the agency's security policies, procedures, and practices, and evaluated the technical security controls over 24 CDC systems. These included 10 key systems, 8 of which were mission-essential, that (1) collect, process, and maintain private or potentially sensitive proprietary business, medical, and personally identifiable information; (2) are essential to CDC's mission; (3) could have a catastrophic or severe impact on operations if compromised; or (4) could be of particular interest to potential adversaries. We also selected 14 general support systems that were part of the network infrastructure supporting the 10 systems.

To review CDC's information security program, we had examined security policies, procedures, and other documents; analyzed risk assessments, security plans, security control assessments, remedial action plans, and contingency plans for 8 selected mission-essential systems; and interviewed personnel at CDC headquarters. To review controls over the 10 key systems and 14 general support systems, we had examined the agency's network infrastructure and assessed the controls associated with system access, encryption, configuration management, and logging and monitoring. We conducted site visits to two CDC facilities located in Atlanta, Georgia.

To accomplish our second objective—on CDC's actions to address the previously identified security program and technical control deficiencies and related recommendations—we requested that the agency provide a status report of its actions to implement each recommendation we made in the June 2018 report. For each recommendation that CDC indicated it had implemented as of August 3, 2018, we examined supporting documents, observed or tested the associated security control or procedure, and/or interviewed the responsible agency officials to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve the underlying control deficiency. Based on this assessment and CDC status reports, we categorized the status of each recommendation as being closed-implemented, open-partially implemented, or open-not implemented. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from December 2016 to December 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

CDC—an operating division of the Department of Health and Human Services (HHS)—serves as the national focal point for disease prevention and control, environmental health, and promotion and education activities designed to improve the health of Americans. The agency is also responsible for leading national efforts to detect, respond to, and prevent illnesses and injuries that result from natural causes or the release of biological, chemical, or radiological agents.

To achieve its mission and goals, the agency relies on an array of partners, including public health associations and state and local public health agencies. It collaborates with these partners on initiatives such as monitoring the public's health, investigating disease outbreaks, and implementing prevention strategies. The agency also uses its staff located in foreign countries to aid in international efforts, such as guarding against global diseases. Table 1 describes the organization of CDC.

Table 1: Organization of the Centers for Disease Control and Prevention (CDC)

CDC Organization	Description
Office of the Director	Guides agency priorities and activities; coordinates program, science, policy, and communications across CDC; and coordinates administrative management activities.
Deputy Director for Infectious Diseases	Leads, promotes, and facilitates science, programs, and policies to reduce the burden of infectious diseases, both domestically and globally. This office includes the National Center for Emerging and Zoonotic Infectious Diseases; the National Center for HIV/AIDS, Viral Hepatitis, Sexually Transmitted Diseases, and Tuberculosis Prevention; and the National Center for Immunization and Respiratory Diseases.
Deputy Director for Non-Infectious Diseases	Reduces the burden of non-infectious diseases, injuries, birth defects, disabilities, and environmental health hazards. This office includes the National Center on Birth Defects and Developmental Disabilities, the National Center for Chronic Disease Prevention and Health Promotion, the National Center for Environmental Health/Agency for Toxic Substances and Disease Registry, and the National Center for Injury Prevention and Control.
Deputy Director for Public Health Science and Surveillance	Leads, promotes, and facilitates science, surveillance, standards, and policies to reduce the burden of diseases, both domestically and globally. This office includes the Office of Science; the Office of Laboratory Science and Safety; the Center for Surveillance, Epidemiology, and Laboratory Services; and the National Center for Health Statistics.
Deputy Director for Public Health Service and Implementation Science	Leads, promotes, and facilitates science, programs and policies to identify and respond to public health threats, both domestically and internationally. It includes the Office of Minority Health and Health Equity; the Center for Global Health; the Center for Preparedness and Response; and the Center for State, Tribal, Local, and Territorial Support.
National Institute for Occupational Safety and Health	Provides leadership to prevent workplace injuries and illness by conducting scientific research, developing guidance and recommendations, sharing information, and responding to requests for workplace health hazard evaluations.

Source: CDC. | GAO-19-70

CDC is staffed by approximately 20,000 employees across the United States and around the world. For fiscal year 2017, according to agency officials, the agency's total appropriation was approximately $12 billion, of which it reported spending approximately $424 million on information technology. In addition, the officials stated that approximately $31 million (or about 7.3 percent of the amount spent on information technology) was for information security across all CDC information technology investments.

CDC Relies on Information Systems to Help Achieve Its Mission

CDC relies extensively on information technology to fulfill its mission and support related administrative needs. Among the approximately 750 systems reported in its inventory, the agency has systems dedicated to supporting public health science, practice, and administration. All of these systems rely on an information technology infrastructure that includes network components, critical servers, and data centers.

CDC Has Defined Organizational Security Roles and Responsibilities

At CDC, the chief information officer (CIO) is responsible for establishing and enforcing policies and procedures protecting information resources. The CIO is to lead the efforts to protect the confidentiality, integrity, and availability of the information and systems that support the agency and its operations, and is to report quarterly to the HHS CIO on the overall effectiveness of CDC's information security and privacy program, including the progress of remedial actions.

The CIO designated a chief information security officer (CISO), who is to oversee compliance with applicable information security and privacy requirements of the agency. The CISO, among other things, is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, and disruption of information and information systems that support the operations and assets of the agency.

To further ensure information security compliance, information systems security officers (ISSO) are responsible for managing the information security program within their respective organizations and report on security program matters to the CISO, including computer security-related incidents. ISSO responsibilities include ensuring that vendor-issued security patches are expeditiously installed and that system owners establish processes for timely removal of access privileges when a user's system access is no longer necessary. In addition, security stewards are to perform operational security analyses supporting the efforts of the ISSO. Further, business stewards serve as program managers, accepting full accountability for the operations of the systems and ensuring that security is planned, documented, and properly resourced for each aspect of the information security program.

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

The *Federal Information Security Modernization Act* (FISMA) of 2014[3] provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA assigns responsibility to the head of each agency 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. In addition, FISMA requires agencies to comply with National Institute of Standards and Technology (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

[3] 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.

the nation.[4] NIST FIPS 200[5] requires agencies to meet minimum security requirements by selecting the appropriate security controls, as described in NIST Special Publication (SP) 800-53.[6] This NIST publication provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets.[7] 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[8] requiring agencies to immediately begin using NIST's Cybersecurity Framework[9] for managing their cybersecurity risks. The framework, which provides guidance for cybersecurity activities, is based on five core security functions:

[4] The potential impact of a loss is categorized as one of three impact levels: 1) low – limited impact; 2) moderate – serious impact; and 3) high – severe or catastrophic impact. 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).

[5] 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).

[6] 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).

[7] 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.

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

[9] 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 the prior administration, *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.

- **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.[10]
- **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 5 functions occur concurrently and continuously, and provide a strategic view of the life cycle of an organization’s management of cybersecurity risk. Within the 5 functions are 23 categories and 108 subcategories that include controls for achieving the intent of each function.[11] Appendix II provides a description of the framework categories and subcategories of controls.

Security Control Deficiencies Placed Selected CDC Systems at Risk

We reported in June 2018 that CDC had implemented numerous controls over the 24 systems we reviewed, but had not always effectively implemented controls to protect the confidentiality, integrity, and availability of these systems and the information maintained on them.

[10] According to the National Institute of Standards and Technology, a cybersecurity event is defined as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

[11] 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 the National Institute of Standards and Technology’s Special Publication 800-53.

Deficiencies existed in the technical controls[12] and agency-wide information security program[13] that were intended to (1) identify risk, (2) protect systems from threats and vulnerabilities, (3) detect cybersecurity events, (4) respond to these events, and (5) recover system operations. These deficiencies increased the risk that sensitive personally identifiable and health-related information, including information regarding the transfer of biological agents and toxins dangerous to public health, could be disclosed or modified without authorization. As shown in table 2, deficiencies existed in all 5 core security function areas for the selected systems we reviewed.

Table 2: Number of GAO-Identified Technical Control and Information Security Program Deficiencies at the Centers for Disease Control and Prevention and Associated Recommendations by Core Security Function

Core security function	Number of technical control deficiencies	Number of technical control recommendations	Number of information security program deficiencies	Number of information security program recommendations
Identify	0	0	5	5
Protect	85	161	1	1
Detect	8	18	3	3
Respond	1	5	1	1
Recover	0	0	1	1
Total	**94**	**184**	**11**	**11**

Source: GAO. | GAO-19-70

CDC Had Identified Risk and Developed Policies and Plans, but 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. These controls include identifying and assessing cybersecurity risk and

[12] According to the National Institute of Standards and Technology, the technical controls (i.e., safeguards or countermeasures) for an information system are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. We also included physical security at data processing facilities as technical controls.

[13] The information security program includes processes, procedures, and practices used to manage the security of information systems.

establishing information security policies, procedures, and plans. We reported in June 2018 that, although CDC had taken steps to implement these controls, it had not (1) categorized the risk-related impact of a key system, identified threats, or reassessed risk for systems or facilities when needed; (2) sufficiently documented technical requirements in policies, procedures, and standards; and (3) described intended controls in facility security plans.

CDC Did Not Appropriately Categorize at Least One Key System, but Assessed Risk to Some Extent at System and Entity-wide Levels

CDC Categorized Systems Based on Potential Impact of Compromise, but Did Not Appropriately Categorize a Key General Support System

As discussed earlier, 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. For networks and other general support systems, NIST SP 800-60[14] notes that the categorization should be based on the high water mark[15] of supported information systems, and on the information types processed, transmitted across the network, or stored on the network or support system. Further, CDC's architecture design principles state that high-impact systems are to be maintained on dedicated machinery and be physically and logically secured from lower-risk systems.

CDC had categorized the 24 systems we reviewed, but the assigned impact level was not always appropriate. In this regard, the agency did not ensure that high-impact systems were logically secured from a lower-

[14] National Institute of Standards and Technology, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*, Special Publication 800-60, Revision 1 (Gaithersburg, MD: August 2008).

[15] For an information system, the potential security impact levels assigned to each of the respective security objectives (confidentiality, integrity, availability) are the highest level (i.e., high water mark) for any one of these objectives that has been determined for the types of information resident on the information system. For example, if confidentiality is considered high impact, integrity moderate impact, and availability low impact, the system should be categorized as a high-impact system based on confidentiality being the highest level of the three objectives.

risk system. Specifically, seven selected high-impact systems relied on a general support system that the agency had categorized as a moderate-impact system (i.e., a lower-risk system). As a result, the high-impact systems were relying on controls in a less secure environment. Officials from the Office of the Chief Information Officer (OCIO) explained that the categorization of the supporting system was outdated based on changes to the agency's operating environment and that they planned to re-evaluate the assigned impact level.

CDC Assessed Risk at the System Level, but Did Not Assess Threats, Document Risk-based Decisions, or Reassess Risk When Needed

According to NIST SP 800-30,[16] risk is determined by identifying potential threats to an organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. NIST also states that assessments should be monitored on an ongoing basis to keep current on risk-impacting changes to the operating environment.

CDC had developed system-level risk assessments for the 8 selected mission-essential systems, and had summarized its risks in a risk assessment report. However, only two of the eight risk assessments had identified potential threats, and only one of these assessments determined the likelihood and impact of threats to that system.

Further, CDC had not always documented risks associated with less secure configuration settings or monitored its assessments to address changes to the operating environment. For example, among the 94 technical control deficiencies that we identified for the 24 systems we reviewed, OCIO officials stated that the agency had not implemented controls for 20 deficiencies due to technical constraints.[17] However, CDC did not address risks associated with decisions not to implement controls for these reasons in the system risk assessments.

[16] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, MD: September 2012).

[17] A technical constraint could include, for example, implementing a control potentially causing functionality problems with legacy applications.

OCIO officials also partially attributed 5 of the 94 technical control deficiencies to new cybersecurity threats and to threat vectors that turned initially sound architecture decisions into vulnerabilities. However, CDC had not addressed such changes in the risk assessments for the affected systems. By not assessing threats or the likelihood of their occurrence and impact and by not documenting the risks, CDC cannot have assurance that appropriate controls are in place commensurate with the level of risk.

CDC Had a Process in Place to Assess Risk to Systems from an Entity-wide Perspective

Beyond the system level, newly discovered threats or vulnerabilities may require an agency to make risk decisions from an entity-wide perspective. An entity-wide perspective is needed because the threats and vulnerabilities may affect more than specific systems.

CDC had a process in place to assess risk from an entity-wide perspective. This process included regular meetings among OCIO and program office staff to discuss policy, threats, and incidents. Specifically, ISSOs held monthly meetings as a continuous monitoring working group to discuss policy updates. In addition, an OCIO official held quarterly briefings that included presentations on incident response tools, incident statistics, and potential threats. OCIO officials also held ad hoc meetings, as necessary, regarding vulnerability and threat concerns when the agency received email alerts from the Federal Bureau of Investigation, the Department of Homeland Security (DHS), or HHS.

CDC Had Not Updated Facility Risk Assessments

In addition to assessing risks for systems, agencies are to assess the risk to their facilities. The Interagency Security Committee (ISC)[18] requires agencies to determine the security level for federal facilities, and to conduct risk assessments at least once every 5 years for Level I and

[18] 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.

Level II facilities and at least once every 3 years for Level III, Level IV, and Level V facilities.[19]

However, the two facility risk assessments that we reviewed had not been updated in a timely manner.[20] Specifically, the risk assessments, covering Level III and Level IV facilities that house the 24 reviewed systems, had been last updated in January 2009 and March 2014—8 years earlier and just over 3 years earlier, at the time of our review in July 2017.

According to a CDC physical security official, the agency had previously relied on a third-party assessor to perform the assessments. The official also said that the agency planned to conduct its own facility risk assessments and had recently developed procedures for conducting these assessments. Until it performs these assessments, CDC may not be aware of new risks to its facilities or the controls needed to mitigate the risks.

CDC Had Documented Controls in Policies, Procedures, and Standards, but Had Not Included Certain Technical Requirements

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes policies and procedures that (1) are based on a risk assessment, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements. According to NIST SP 800-53, an agency should develop policies and procedures for each of the 18 NIST families of security controls to facilitate the implementation of the controls.

CDC had documented numerous policies, procedures, and standards that addressed each of the 18 control families identified in NIST SP 800-53.

[19] The facility security level is a categorization that ranges from Level I (lowest risk) to Level V (highest risk) based on the analysis of security-related factors, such as symbolism, population (e.g., employees and visitors), and size. The facility security level serves as the basis for identifying countermeasures that should be implemented at federal facilities to reduce the level of risk to an acceptable level.

[20] We reviewed two facility risk assessments because these two assessments covered facilities housing resources for the eight selected systems.

For example, the agency had developed policies and procedures governing physical access to CDC facilities, role-based training of personnel with significant security responsibilities, security assessment and authorization of systems, and continuity of operations, in addition to standard operating procedures that covered numerous other controls.

The agency had also developed the *CDC IT Security Program Implementation Standards*, which describes the agency's security program requirements and minimum mandatory standards for the implementation of information security and privacy controls. In addition, the agency had documented configuration standards, which specified minimum configuration settings, for devices such as firewalls, routers, switches, as well as Unix and Windows servers.

However, these policies and standards sometimes lacked the technical specificity needed to ensure controls were in place. To illustrate, the agency had not sufficiently documented detailed guidance or instructions to address numerous technical control deficiencies we identified, such as insecure network devices, insecure database configurations, not blocking certain email attachments, and not deploying a data loss prevention capability.

According to OCIO officials, the agency's periodic reviews and updates to existing cybersecurity policies and standards did not reveal and address these issues. Nevertheless, without clear and specific guidance or instructions for implementing technical controls, the agency had less assurance that controls were in place and operating as intended.

CDC Had Identified and Updated Controls in System Security Plans Annually, but Had Not Developed Facility Security Plans

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 states that plans should be reviewed and updated to ensure that they continue to reflect the correct information about the systems, such as changes in system owners, interconnections, and authorization status, among other things.

HHS and CDC policies require that such plans be reviewed annually. In addition, the ISC requires that agencies develop and implement an operable and effective facility security plan. CDC standards require the organization to prepare a facility security plan (or similar document).

CDC had developed security plans for the 8 selected mission-essential systems. With a few exceptions, the plans addressed the applicable security controls for those systems.[21] The agency also had reviewed and updated the plans annually.

However, CDC had not developed security plans for the facilities housing resources for the selected systems. Physical security officials stated that they had not developed security plans because they did not have a sufficient number of staff to develop them. Without comprehensive security plans for the facilities, CDC's information and systems would be at an increased risk that controls to address emergency situations would not be in place and personnel at the facilities would not be aware of their roles and responsibilities for implementing sound security practices to protect systems housed at these CDC locations.

CDC Had Implemented Controls Intended to Protect Its Systems, but Deficiencies Existed

The *protect* core security function is intended to help agencies develop and implement the appropriate safeguards for their systems to ensure achieving the agency's mission and to support the ability to limit or contain the impact of a potential cybersecurity event. Controls associated with this function include 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 CDC had implemented controls that were intended to protect its operating environment, we reported in June 2018 that the agency did not consistently (1) implement access controls effectively, (2) encrypt sensitive data, (3) configure devices securely or apply patches in

[21] We determined that, of the approximately 2,800 total controls listed in the security plans for the 8 selected mission-essential systems, CDC had not provided detailed implementation information for 57 of the controls (or about 2 percent).

a timely manner, or (4) ensure staff with significant security responsibilities received role-based training.

CDC Did Not Consistently Implement Effective Access Controls

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, limit, and detect 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. However, CDC had not consistently implemented these controls.

CDC Implemented Enterprise-wide Identification and Authentication Controls, but Did Not Consistently and Securely Configure Password Controls for Certain Accounts on Devices and Systems

NIST SP 800-53 states that agencies should implement multi-factor authentication for their users of information systems. Multi-factor authentication involves using two or more factors to achieve authentication. A factor is something you know (password or personal identification number), something you have (token and personal identity verification (PIV) card), or something you are (biometric). Also, NIST and CDC policy state that information systems shall have password management controls established to include minimum password complexity requirements, password lifetime restrictions, prohibitions on password reuse, and user accounts temporarily locked out after a certain number of failed login attempts during a specified period of time.

CDC had applied enterprise-wide solutions to ensure appropriate identification and multi-factor authentication of its general user community through, for example, the use of PIV cards. However, instances of weak password management controls existed for certain accounts on network devices, servers, and database systems. According to OCIO officials, password control deficiencies existed primarily due to technical constraints, administrators not being aware of technical requirements, or administrators not adequately monitoring configuration settings. Without more secure password settings, CDC’s information and systems are at an increased risk that unauthorized individuals could have guessed passwords and used them to obtain unauthorized access to agency systems and databases.

CDC Authorized Users More Access than Needed to Perform Their Jobs

NIST SP 800-53 states that agencies should employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks. It also states that privileged accounts—those with elevated access permissions—should be strictly controlled and used only for their intended administrative purposes.

CDC had implemented controls intended to ensure that users were granted the minimum level of access permissions necessary to perform their legitimate job-related functions. However, the agency had granted certain users more access than needed for their job functions, including excessive access permissions on a key server.

According to OCIO officials, CDC systems had deficiencies related to restricting access primarily due to technical constraints or administrators not adequately monitoring configuration settings. By not appropriately restricting access, CDC's information and systems are at an increased risk that individuals could deliberately or inadvertently compromise database systems or gain inappropriate access to information resources.

CDC Did Not Effectively Implement Boundary Controls to Ensure Network Integrity

NIST SP 800-53 states that agencies should control communications at information systems' external boundaries. It states that, to manage risks, agencies should use boundary protection mechanisms to separate or partition computing systems and network infrastructures containing higher-risk systems from lower-risk systems.[22]

Although CDC had implemented multiple controls that were designed to protect system boundaries, the agency had not sufficiently separated higher-risk systems from lower-risk systems. According to OCIO officials, deficiencies in boundary protection controls existed due to new

[22] Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices connected to a network. Implementing multiple layers of security to protect an information system's boundaries can reduce the risk of a successful cyberattack. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection technologies can be deployed to defend against attacks from the Internet.

cybersecurity threats turning initially sound architecture decisions into vulnerabilities, technical constraints, and administrators not being aware of technical requirements or adequately monitoring configuration settings. Without stronger boundary controls, CDC's information and systems are at an increased risk that an attacker could have exploited these boundary deficiencies and leveraged them to compromise CDC's internal network.

CDC Physically Protected Information System Assets, but Did Not Consistently Ensure Access Remained Appropriate

NIST SP 800-53 states that agencies should implement physical access controls to protect employees and visitors, information systems, and the facilities in which they are located. In addition, NIST states that agencies should review access lists detailing authorized facility access by individuals at the agency-defined frequency. In its standards, CDC requires implementation of the NIST special publication and requires that access lists detailing authorized facility access by individuals be reviewed at least every 365 days.

CDC had implemented physical security controls. The agency had implemented physical security measures to control access to certain areas and to ensure the safety and security of its employees, contractors, and visitors to CDC facilities. For example, CDC had issued PIV cards and Cardkey Proximity Cards to its employees and contractors, and had limited physical access to restricted areas based on the permissions it granted via these cards.

However, the agency had not consistently reviewed authorized access lists. In this regard, CDC did not have a process in place for periodically reviewing the lists of individuals with access to rooms containing sensitive resources to ensure that such access remained appropriate. Without reviewing authorized access lists, CDC has reduced assurance that individual access to its computing resources and sensitive information is appropriate.

CDC Had Not Consistently Encrypted Sensitive Authentication Data

NIST SP 800-53 states that agencies should encrypt passwords both while stored and transmitted, and configure information systems to establish a trusted communication path between the user and the system.

Additionally, NIST requires that, when agencies use encryption, they use an encryption algorithm that complies with FIPS 140-2.[23]

CDC had used FIPS-compliant encryption for its PIV card implementation, but had not effectively implemented encryption controls in other areas. According to OCIO officials, encryption control deficiencies existed primarily due to technical constraints, administrators not being aware of a technical solution, or configuration settings not being adequately monitored. By not using encryption effectively, CDC limits its ability to protect the confidentiality of sensitive information, such as passwords.

CDC Had Not Consistently Configured Servers Securely or Applied Patches in a Timely Manner

NIST SP 800-53 states that agencies should disable certain services with known security vulnerabilities. This includes configuring security control settings on operating systems in accordance with publicly available security checklists (or benchmarks) promulgated by NIST's National Checklist Program repository. This repository contains, for example, the security configuration benchmarks established by the Center for Internet Security (CIS) for Windows servers.

NIST also states that agencies should test and install newly-released security patches, service packs, and hot fixes in a timely manner. In addition, CDC policy required that software patches for remediating vulnerabilities designated as critical or high risk be applied to servers within 45 days of being notified that a patch is available or within 7 days of when an exploit is known to exist. Further, agency policy specified that administrators configure Windows servers in accordance with the CDC-approved security benchmarks.

CDC had documented security configuration baselines, but had not always securely configured its systems or applied patches. In addition, the agency had not consistently configured security settings in accordance with prescribed security benchmarks or applied patches in a timely manner. For example:

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

- CDC had configured Windows servers to run unnecessary services.
- CDC had configured only about 62 percent of the security settings in accordance with prescribed benchmark criteria on the Windows and infrastructure servers supporting five systems that we reviewed.
- During our site visit in April 2017, CDC had not installed 21 updates on about 20 percent of the network devices, including 17 updates that the vendor considered to be critical or high-risk. The oldest of the missing updates dated back to January 2015.
- CDC had not updated database software supporting two selected systems to a more recent version that addressed vulnerabilities with a medium severity rating.

According to OCIO officials, CDC had deficiencies in configuration and patching primarily due to administrators not being aware that there was a technical solution or did not adequately monitor configuration settings. By not securely configuring devices and installing updates and patches in a timely manner, the agency is at increased risk that individuals could have exploited known vulnerabilities to gain unauthorized access to agency computing resources.

Staff Received Security Awareness Training, but At Least 15 Percent of Those with Significant Security Responsibilities Did Not Receive Role-Based Training

According to NIST SP 800-53, agencies should provide adequate security training to individuals in a role such as system/network administrator and to personnel conducting configuration management and auditing activities, tailoring the training to their specific roles. In addition, one of the cybersecurity cross-agency priority goals requires that agencies implement training that reduces the risk that individuals will introduce malware through email and malicious or compromised web sites.[24]

Consistent with NIST SP 800-53, CDC policy required network users to receive annual security awareness training. Accordingly, for fiscal year

[24] Cybersecurity cross-agency priority goals were established by the prior administration as part of implementing the requirement in the *Government Performance and Results Act Modernization Act of 2010* to develop federal government priority goals for information technology management. Sec. 5, Pub. L. No. 111-352 (Jan. 4, 2011); 124 Stat. 3866, 3873; 31 U.S.C. § 1120(a)(1)(B).

2017, all CDC staff completed the required annual security awareness training.

CDC policy also required that those staff identified as having significant security responsibilities receive role-based training every 3 years. However, not all staff with significant security responsibilities received role-based training within the defined time frames. The agency used a tracking system to monitor the status of role-based training for 377 individuals who had been identified as having significant security responsibilities. As of May 2017, 56 (about 15 percent) of the 377 individuals had not completed the training within the last 3 years, and 246 (about 65 percent) of them had not taken training within the last year.

In addition, CDC had not identified at least 30 other staff with significant security responsibilities who required role-based training. Specifically, none of the 18 security and database administrators for four selected systems were included among the individuals being tracked, although these administrators had significant security responsibilities. Further, the agency provided us with a list of 42 individuals whose job series indicated that they required role-based training. However, 12 of the 42 were not included among the tracked individuals. Furthermore, given the number of deficiencies identified and the rapidly evolving nature of cyber threats, CDC’s requirement that staff take role-based training only once every 3 years is not sufficient for individuals with significant cybersecurity responsibilities.

According to OCIO officials, managers are responsible for identifying those individuals with significant security responsibilities. The process used to track training was manual and required an individual’s manager to specify training requirements. The officials noted that the agency plans to implement a new HHS annual role-based training requirement in fiscal year 2018 and that they intend to work to enhance oversight as the new requirement is implemented.[25]

The officials also stated that at least 10 of the 94 technical control-related deficiencies identified in our June 2018 report had resulted, at least in part, from staff not being aware of control requirements or solutions to address the deficiencies. As a result, CDC’s information and systems are

[25] Since the issuance of the June 2018 report, CDC has updated their role-based training requirement from once every three years to annually.

at increased risk that staff may not have the knowledge or skills needed to appropriately protect them.

CDC Had Not Effectively Implemented Controls Intended to Detect Incidents or Deficiencies

The *detect* core security function is intended to allow for the timely discovery of cybersecurity events. Controls associated with this function include logging and monitoring system activities and configurations, assessing security controls in place, and implementing continuous monitoring. In June 2018, we reported that, although CDC had implemented controls intended to detect the occurrence of a cybersecurity event, it had not sufficiently implemented logging and monitoring capabilities or effectively assessed security controls.

CDC Had Implemented Limited Logging and Monitoring Capabilities

NIST SP 800-53 states that agencies should enable system logging features and retain sufficient audit logs to support the investigations of security incidents and the monitoring of select activities for significant security-related events. In addition, National Archives and Records Administration records retention guidance states that system files containing information requiring special accountability[26] that may be needed for audit or investigative purposes should be retained for 6 years after user accounts have been terminated or passwords altered, or when an account is no longer needed for investigative or security purposes, whichever is later.[27] NIST also states that agencies should monitor physical access to facilities where their information systems reside to detect physical security incidents. Further, NIST SP 800-53 states that agencies should monitor and control changes to configuration settings.

Although CDC had implemented centralized logging and network traffic monitoring capabilities, the capabilities were limited. For example, the agency's centralized logging system used for security monitoring had a

[26] Files containing information requiring special accountability are user identification records associated with systems which are highly sensitive and potentially vulnerable.

[27] National Archives and Records Administration, *General Records Schedule 3.2: Information Systems Security Records*, Transmittal 26 (Washington D.C.: September 2016).

limited storage capacity and did not meet the National Archives and Records Administration requirements. In addition, CDC had not centrally collected and monitored security event data for many key assets connected to the network. As a result, increased risk existed that CDC would not have been able to detect anomalous activities that may have occurred from malware attacks over time. OCIO officials stated that, as a compensating measure, the agency prevents direct communications between workstations. However, such a measure does not allow the agency to detect potentially inconsistent activities that may have occurred from malware attacks within the same data center.

CDC also had not consistently reviewed physical access logs to detect suspicious physical access activities, such as access outside of normal work hours and repeated access to areas not normally accessed. Program offices responsible for 7 of the 8 selected mission-essential systems did not conduct such a review. According to OCIO officials, the offices were not aware of the need for a review. However, without reviewing physical access logs, CDC has reduced assurance that the agency would detect suspicious physical access activities.

Further, CDC had not routinely monitored the configuration settings of its systems to ensure that the configurations were securely set. For example, for at least 41 of 94 technical control deficiencies we identified, OCIO officials cited quality control gaps where the change management process or system administrators had not discovered deficiencies resulting from insecure configuration settings. Without an effective monitoring process in place for system configurations, the agency was not aware of insecure system configurations.

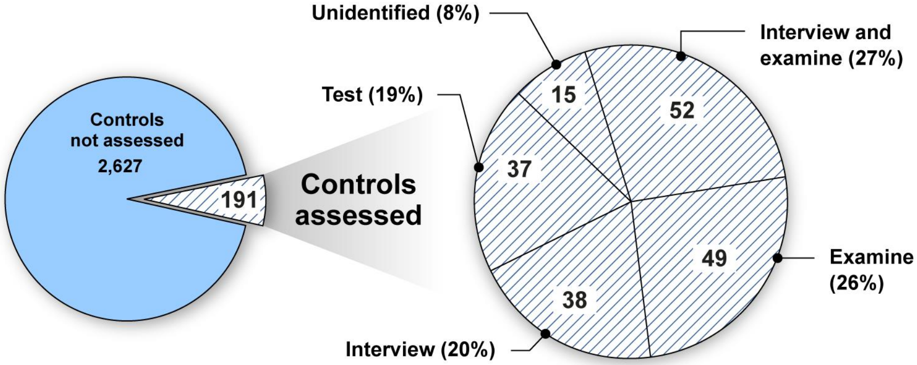
CDC Did Not Effectively Test or Assess Controls to Detect Deficiencies

FISMA requires each agency to periodically test and evaluate the effectiveness of its information security policies, procedures, and practices. The law also requires agencies to test the management, operational, and technical controls for every system identified in the agency's required inventory of major information systems at a frequency depending on risk, but no less than annually. In addition, NIST SP 800-53A identifies three assessment methods—interview, examine, and test—

and describes the potential depth and coverage for each.[28] Assessing a control's effectiveness based on an interview is likely less rigorous than examining a control; similarly, examining a control is likely less rigorous than testing the control's functionality.

CDC had not sufficiently tested or assessed the effectiveness of the security controls for the 8 mission-essential systems that we reviewed. Although CDC annually assessed security controls of selected systems, the agency had only examined control descriptions in security plans to ensure accuracy. At least once every 3 years, the agency selected controls for a more in-depth assessment of the 8 mission-essential systems we reviewed. However, CDC had assessed only 191 (about 7 percent) of 2,818 controls described in the security plans for the selected systems. In addition, the agency used methods for assessing controls that were often not rigorous enough to identify the control deficiencies that we identified. For example, as depicted in figure 1, CDC relied exclusively on interviews—a less rigorous method—to assess 20 percent of the 191 controls it assessed for the selected systems.

Figure 1: Methods Used by the Centers for Disease Control and Prevention to Assess Security Controls



Source: GAO analysis of selected system assessments. | GAO-19-70

[28] According to NIST, the interview method is the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, achieve clarification, or obtain evidence. The test method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

The security control tests and assessments were insufficient in part because CDC had not developed comprehensive security assessment plans or had not consistently implemented the plans for the 8 selected mission-essential systems we reviewed. For example, one system's assessment plan indicated that five controls should be assessed using a testing methodology; instead, however, the assessor conducted interviews to determine whether controls were effective or not.

OCIO officials stated that the security control test and assessment process is manual and staffing is limited. They stated that the agency intends to rely increasingly on automated tools—such as the tools implemented by the Continuous Diagnostics and Mitigation program—for performing the assessments. Nevertheless, by not assessing controls in an in-depth and comprehensive manner, CDC has limited assurance that the security controls are in place and operating as intended. Further, without developing and implementing comprehensive assessment plans, assessments may not be performed with sufficient rigor to identify control deficiencies.

CDC Had Implemented Processes for Responding to Incidents or Identified Deficiencies, but Did Not Always Take Timely Corrective Actions

The *respond* core security function is intended to support the ability to contain the impact of a potential cybersecurity event. Controls associated with this function include implementing an incident response capability and remediating newly-identified deficiencies. Although CDC had implemented controls for incident response to detect cybersecurity events, we reported in June 2018 that the agency had not maintained adequate information to support its incident response capability or taken timely corrective actions to remediate identified control deficiencies.

CDC Had Implemented Incident Response Capabilities, but Did Not Maintain Adequate Information

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, and keep them updated according to agency requirements. 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.

Further, NIST states that agencies are to monitor incidents by tracking and documenting them and maintain records about each incident, including forensic analysis. Finally, National Archives and Records Administration guidance states that records and data relevant to security incident investigations should be retained for 3 years.

CDC had implemented an incident response capability. The agency had developed policy, procedures, and a plan that addressed incident response, and updated them annually. CDC had an incident response team that managed all of the incident handling and response efforts for the agency, and conducted forensic analyses for reported security incidents. Team members had undergone training, such as an advanced network forensic and analysis course offered by a private firm. In addition, the agency had periodically tested its incident handling capability by conducting penetration testing exercises. These exercises allowed the team to test its real-time response capabilities.

CDC's incident response procedures state that incident tickets should include a description of actions taken, response time, and whether actions have been completed or not. The agency's procedures also require that computers affected by an incident be removed from the network immediately.

Nevertheless, CDC had shortcomings in implementing its incident response capability and monitoring procedures. For the 11 security incidents CDC considered most significant over a 19-month period ending in March 2017,[29] the agency had not consistently described the actions taken, the response times, or whether remedial actions had been completed. The agency also had not maintained audit log records for its security incidents. For example, the agency described recommended actions for 10 of the 11 incidents, but did not describe the actions that had been taken.

In addition, although incident response team officials told us that all incident ticket records had been saved, CDC had not retained system log

[29] We conducted our initial site visit to assess incident response capabilities during the week of March 7, 2017.

data that supported incident resolution for at least five of the incidents. The agency's policy did not address record retention in accordance with National Archives and Records Administration guidance. Further, for two of the security incidents, the security incident tickets did not clearly indicate when two compromised workstations had been removed from the network. According to OCIO officials, shortcomings in fully documenting incidents resulted from the organization being understaffed, primarily due to budget limitations and the inability to hire qualified personnel. Without effectively tracking and documenting information system security incidents, CDC's systems are at increased risk that the impact of security incidents would not be fully addressed.

CDC Had Remedial Action Plans to Address Identified Deficiencies for Selected Systems, but Did Not Always Take Timely Corrective Actions or Have Plans for Other Needed Corrective Actions

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, or practices. NIST SP 800-53 states that agencies are to develop a plan of action and milestones (POA&M) for an information system to document the agency's planned remedial actions to correct identified deficiencies. CDC policy was consistent with the NIST guidelines.

CDC had developed POA&Ms for deficiencies identified by its security control assessments, but had not remediated the deficiencies in a timely manner. For each of the 8 selected mission-essential systems, the agency had created plans for correcting control deficiencies. However, the agency did not implement several remedial actions by their due date. For example, expected completion dates had passed for correcting deficiencies associated with 4 of the 8 selected mission-essential systems. For these 4 systems, the completion dates were 1 to 8 months beyond the due dates at the time of our review in September 2017.

According to Office of the Chief Information Security Officer officials, program offices that own the systems did not always communicate updates on the status of remedial actions for their respective systems, noting that deficiencies may have been corrected. Without effective communication to update its POA&Ms, CDC was not in a position to effectively manage its remedial actions and correct known deficiencies in a timely manner.

CDC Had Developed and Tested Plans for System Recovery, but Had Not Assessed the Risk Associated with the Close Proximity of an Alternate Processing Site

The *recover* core security function 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 electronically maintained 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.

NIST SP 800-53 states that agency systems should have a contingency plan that includes the identification of key personnel and the systems' essential mission functions and addresses full information system restoration. For high-impact systems, NIST specifies that agencies test contingency plans at an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. In addition, NIST states that organizations should initiate corrective actions based on testing if they are needed.

As we reported in June 2018, CDC had developed and fully tested contingency plans for each of the 8 selected mission-essential systems that we reviewed. Each plan identified key personnel and their contact information, essential mission functions of the systems, and instructions on how to fully restore the systems in the event of a disruption. Additionally, between January 2015 and May 2017, CDC had tested whether the 8 systems could be recovered at their respective alternate sites, and had initiated corrective actions based on the results of the tests.

However, the alternate site for 6 of the 8 selected mission-essential systems was located in relatively close proximity to the main processing site. Although 2 systems had alternate sites located in another state, the alternate site for the other 6 systems was within the same metropolitan area. As a result, an event such as a natural disaster or substantial power outage could affect both the main and alternate sites for these systems, potentially rendering CDC unable to complete functions associated with its mission. Prompt restoration of service is necessary because the required recovery time for these systems ranged from 4 to 24 hours.

Security plans for 3 of the systems recognized the hazards of having the sites within the same geographical region, but stated that CDC had accepted this risk. According to OCIO officials, having a site further away was cost prohibitive; however, the officials had not documented this analysis or the associated risk of having the agency's processing sites located within the same geographical area. Without documenting the analysis and associated risk, CDC had less assurance that senior leadership was aware of the risk of agency systems being unavailable. As a consequence, senior leadership may not agree whether acceptance of the risk was warranted.

CDC Had Not Consistently or Effectively Implemented Elements of Its Information Security Program

An underlying reason for the information security deficiencies in selected systems was that, although the agency had developed and documented an agency-wide information security program, it had not consistently or effectively implemented elements of the program. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes the following elements:

- periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems or group of information systems, as appropriate;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, or practices of the agency; and
- plans and procedures to ensure continuity of operations for information systems.

As discussed previously in this report, CDC had implemented aspects of each of these elements. For example, the agency had conducted risk assessments, developed security plans, assessed security controls, developed remedial action plans, and developed and tested contingency plans for each of the 8 selected mission-essential systems. In addition, the agency had documented numerous policies and procedures and ensured that staff had completed annual security awareness training.

However, CDC's program had shortcomings. For example, as discussed earlier in this report, CDC had not consistently or effectively:

- addressed threats, technical constraints, and the changing threat environment in its system risk assessments, or assessed the risk of having alternate processing sites within close proximity to each other;
- documented detailed technical requirements in policies and procedures, or facility controls in facility security plans;
- tracked and trained staff with significant security responsibilities;
- monitored configuration settings and comprehensively assessed system controls;
- remediated deficiencies in a timely manner; or
- documented its cost analysis and associated risk of having an alternate processing site within the same geographical region as its primary processing site.

Until CDC addresses these shortcomings and consistently and effectively implements all elements of its information security program, the agency will lack reasonable assurance that its computing resources are protected from inadvertent or deliberate misuse.

CDC Has Implemented Many of the Recommendations in Our June 2018 Report and Plans to Implement the Rest

In our June 2018 report,[30] we made 195 recommendations to CDC to strengthen its technical security controls and bolster its agency-wide information security program. Specifically, we recommended that the agency take 184 actions to resolve technical control deficiencies by implementing stronger access controls, encrypting sensitive data, configuring devices securely, applying patches in a timely manner, strengthening firewall rules, and implementing logging and monitoring controls more effectively, among other actions. We also made 11 recommendations for CDC to improve its information security program by, among other things, assessing risks as needed, documenting more detailed technical requirements, monitoring and assessing controls more comprehensively, and remediating deficiencies in a timely manner.

Since the issuance of our June 2018 report, CDC has made significant progress in implementing the recommendations we made to resolve the technical security control deficiencies in the information systems we reviewed and to improve its information security program. In this regard, the agency has implemented many of the recommendations for improving technical security controls for the systems we reviewed and has developed plans to implement recommendations for enhancing its information security program.

Specifically, as of August 3, 2018, CDC had fully implemented 102 (55 percent) of the 184 recommendations we made to fortify the technical security controls over the systems we reviewed. In addition, the agency had partially implemented 20 (11 percent) of the 184 recommendations. In these instances, CDC had made progress toward implementing the recommendations, but had not completed all of the necessary corrective actions for us to close the recommendations. Therefore, these recommendations remain open. Further, CDC did not provide any

[30] GAO-18-437SU.

evidence that it had implemented the remaining 62 technical control-related recommendations.

Table 3 summarizes the status of CDC's efforts to implement the 184 recommendations that we made to resolve the technical control deficiencies, as of August 3, 2018.[31]

[31] We determined that 14 of the implemented, and 9 of the partially-implemented recommendations were either fully or partially addressed due to the decommissioning of one of the mission-essential systems, a key application process, and certain servers selected for this review. In August 2018, while onsite, we reviewed configuration settings—to include the authorization to operate, and change management procedures—to ensure the vulnerabilities were addressed in the new systems and servers.

Table 3: Status of Efforts by the Centers for Disease Control and Prevention to Implement GAO's Technical Control-Related Recommendations by Core Security Function, as of August 3, 2018

Core security function	Number of technical control-related recommendations	Status of Technical Control-related Recommendations		
n/a	n/a	Closed–implemented	Open–partially implemented	Open–not implemented
Identify	0	0	0	0
Protect	161	89	18	54
Detect	18	9	2	7
Respond	5	4	0	1
Recover	0	0	0	0
Totals	**184**	**102**	**20**	**62**

Legend:

Closed-implemented (CDC successfully completed actions to implement the recommendation)

Open-partially implemented (CDC had made progress toward—but has not completed—implementing the recommendation)

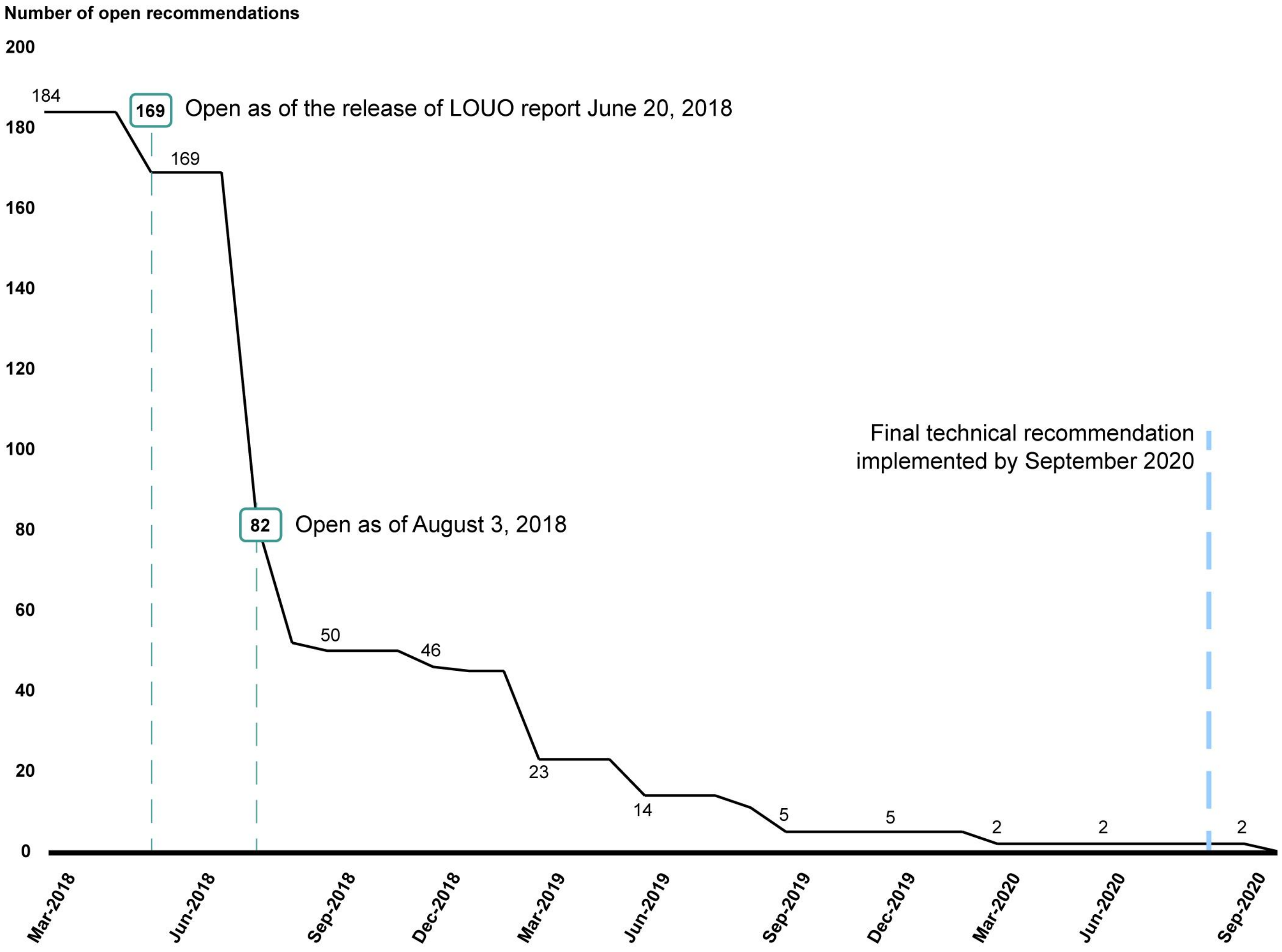
Open-not implemented (CDC has not acted to implement the recommendation)

Source: GAO analysis of CDC data. | GAO-19-70

By implementing 102 recommendations, CDC (as of August 3, 2018) reduced some of the risks associated with certain key activities. Specifically, these efforts included protecting network boundaries and logging and monitoring security events for indications of inappropriate or unusual activity on systems—that we highlighted in our June 2018 report as being particularly vulnerable and requiring the agency's greater priority and attention. In addition, the agency had implemented several of our recommendations to rectify a number of the security control deficiencies. These efforts included strengthening firewall rules, implementing stronger access controls, configuring devices securely, and expanding its audit monitoring capabilities.

In addition, CDC had developed a plan of action and milestones (POA&M) for each of the identified technical control deficiencies and related recommendations that remained open as of August 3, 2018. The POA&Ms assigned organization responsibilities, identified estimated costs, identified points of contact, and established time frames for resolving the deficiencies and closing the related recommendations. The agency's plans called for it to implement the majority of the remaining open technical control-related recommendations by September 2019, and all recommendations by September 2020, as shown in figure 2.

Figure 2: The Centers for Disease Control and Prevention's Planned Timeline for Fully Implementing GAO's Technical Control-Related Recommendations



Source: GAO analysis of Centers for Disease Control and Prevention data. | GAO-19-70

Our June 2018 report also included 11 recommendations to CDC to improve its information security program. In particular, we recommended that the agency, among other things, evaluate system impact level categorizations to ensure they reflect the current operating environment; update risk assessments to identify threats and the likelihood of impact of the threat on the environment; and update the facility risk assessments. In addition, we recommended that the agency take the necessary steps to make sure staff with significant security roles and responsibilities are appropriately identified and receive role-based training; monitor the configuration settings of agency systems to ensure the settings are set as intended; update security control assessments to include an assessment of controls using an appropriate level of rigor; and remediate POA&Ms in a timely manner. Further, we recommended that the agency document the cost-benefit analysis with associated risk of having an alternate site within the same geographical region as the main site.

As of August 3, 2018, the agency had partially implemented 1 of the 11 information security program-related recommendations, but had not provided any evidence that it had implemented the remaining 10 recommendations. Regarding the partially implemented recommendation, CDC had provided role-based training to all personnel performing significant security responsibilities. However, the agency still needed to establish and automate the identification process and the tracking of training records for individuals needing specialized security role-based training. CDC had developed plans to fully implement this recommendation and each of the remaining 10 information security program-related recommendations by July 2019. 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.

Agency Comments

We received written comments on a draft of this report from CDC. In its comments, which are reprinted in appendix III, the agency stated that it recognizes the risks associated with operating a large, global information technology enterprise and has implemented processes, procedures, and tools to better ensure the prevention, detection, and correction of potential incidents. CDC also said cybersecurity remains a high priority and that it takes the responsibilities for protecting public health information and data entrusted to it seriously. To strengthen its cybersecurity program, the agency stated that it is restructuring and streamlining the cyber program and IT infrastructure of its Office of the Chief Information Officer.

Further, CDC stated that it has leveraged GAO's limited official use only report, issued in June 2018, to accelerate its implementation, infrastructure, and software deployments to complete phrases one and two of DHS's Continuous Diagnostics and Mitigation program. The agency also said it concurred with, and highlighted a number of actions that it had planned or begun taking to remediate, the 11 security program recommendations that we made to CDC in our June 2018 report.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Health and Human Services, and the department's Office of the Inspector General, the Director of CDC, 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 Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. GAO staff who made key contributions to this report are listed in appendix IV.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objective was to assess the extent to which CDC 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 2018, we issued a report which detailed the findings from our work in response to this objective.[1] In the report, we made 184 recommendations to CDC to resolve the technical security control deficiencies in the information systems we reviewed and 11 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 2018 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. The appendix contained sensitive details about the technical security control deficiencies in the CDC’s information systems and computer networks that we reviewed, and the 184 recommendations we made to mitigate those deficiencies. We also provided a draft of this report to CDC 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 CDC’s information systems and networks.

In addition, this report addresses a second objective that was not included in the June 2018 report. Specifically, this objective was to determine the extent to which CDC had taken corrective actions to address the previously identified security program and technical control

[1] GAO, *Information Security: CDC Needs to Improve Its Program and Resolve Control Deficiencies*, GAO-18-437SU (Washington, D.C.: June 20, 2018).

deficiencies and related recommendations for improvement that we identified in the earlier report.

As noted in our June 2018 report, we determined the extent to which CDC had effectively implemented an information security program and controls to protect the confidentiality, integrity, and availability of its information on selected information systems. To do this, we initially gained an understanding of the overall network environment, identified interconnectivity and control points, and examined controls for the agency's networks and facilities. We conducted site visits at two CDC facilities in Atlanta, Georgia.

To evaluate CDC's controls over its information systems, we used our Federal Information System Controls Audit Manual,[2] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information. We based our assessment of controls on requirements identified by the Federal Information Security Modernization Act of 2014 (FISMA),[3] which establishes key elements for an effective agency-wide information security program; NIST guidelines and standards;[4] Department of Health and Human Services and CDC policies, procedures, and standards; and standards and guidelines from relevant security organizations, such as

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

[3] *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.

[4] 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).

the National Security Agency, the Center for Internet Security,[5] and the Interagency Security Committee.[6]

We had reviewed a non-generalizable sample of the agency's information systems, focusing on those systems that (1) collect, process, and maintain private or potentially-sensitive proprietary business, medical, and personally identifiable information; (2) are essential to CDC's mission; and (3) were assigned a Federal Information Processing Standard rating of moderate or high impact.[7] Based on these criteria, we had selected eight mission-essential systems for our review.

Of these systems, the agency had categorized 7 as high-impact systems and 1 as a moderate-impact system. For these 8 selected mission-essential systems, we had reviewed information security program-related controls associated with risk assessments, security plans, security control assessments, remedial action plans, and contingency plans.

To assess the safeguards CDC implemented for its systems, we had examined technical security controls for 24 CDC systems,[8] including

[5] The Center for Internet Security is a nonprofit entity that uses a global information technology community to safeguard private and public organizations against cyber threat. We used the Center for Internet Security tool to assess CDC's information systems.

[6] 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.

[7] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 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] Because we examined only 24 of the more than 750 systems CDC reported in its FISMA inventory with FIPS 199 categorizations, the results of our review of system-level controls cannot be generalized to the entire CDC environment.

systems the agency designated as high-value assets.[9] These included 10 key systems, 8 of which were high- and moderate-impact mission-essential systems just described, 1 additional high-impact system, 1 additional moderate-impact system, and 14 general support systems. We selected the additional high-impact system because the agency re-categorized it as a high-impact system during our review. We selected the additional moderate-impact system because the agency used it to control physical access to highly sensitive CDC biologic lab facilities, including facilities that handle dangerous and exotic substances that cause incurable and deadly diseases.

We selected 10 key systems, 8 of which were mission-essential systems, for review that (1) collect, process, and maintain private or potentially sensitive proprietary business, medical, and personally identifiable information; (2) are essential to CDC's mission; (3) could have a catastrophic or severe impact on operations if compromised; or (4) could be of particular interest to potential adversaries. We also selected 14 general support systems that were part of the agency's network infrastructure supporting the 10 key systems.[10]

To review controls over the 10 key systems and 14 general support systems, we had examined the agency's network infrastructure and assessed the controls associated with system access, encryption, configuration management, and logging and monitoring. For reporting purposes, we had categorized the security controls that we assessed into the five core security functions described in the National Institute of

[9] 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.

[10] The 14 general support systems included network devices such as routers, switches, and firewalls; workstations; and servers.

Standards and Technology's (NIST) cybersecurity framework.[11] The five core security functions are:

- **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.
- **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.

These core security functions are described in more detail in appendix II.

For the *identify* core security function, we had examined CDC's reporting for its hardware and software assets; analyzed risk assessments for the eight selected mission-essential systems to determine whether threats and vulnerabilities were being identified; reviewed risk assessments for two facilities; analyzed CDC 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 eight selected systems to determine if those plans had been documented and updated according to federal guidance. We also evaluated the risk assessments for two facilities that housed the 8 mission-essential selected systems.

For the *protect* core security function, we had examined access controls for the 24 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

[11] 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 the prior administration, *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.

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

We also had examined configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted. In addition, we had 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 had 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.

For the *detect* core security function, we had analyzed centralized logging and network traffic monitoring capabilities for key assets connected to the network; analyzed CDC's procedures and results for assessing security controls to determine whether controls for the eight selected mission-essential systems had been sufficiently tested at least annually and based on risk. We also had 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 the *respond* core security function, we had reviewed CDC's implementation of incident response practices, including an examination of incident tickets for 11 incidents; and had examined the agency's process for correcting identified deficiencies for the eight selected mission-essential systems.

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

Within the core security functions, as appropriate, we had evaluated the elements of CDC'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 8 selected mission-essential systems. In addition, we had assessed whether the agency had ensured staff had completed security awareness training and whether those with significant security responsibilities received commensurate training. We also had evaluated CDC's security policies and procedures.

To determine the reliability of CDC's computer-processed data for training and incident response records, we had 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 a combination of methods, we concluded that the data were sufficiently reliable for the purposes of our work.

To accomplish our second objective—on CDC's actions to address the previously identified security program and technical control deficiencies and related recommendations[12]—we requested that the agency provide a status report of its actions to implement each of the recommendations. For each recommendation that CDC indicated it had implemented as of August 3, 2018, we examined supporting documents, observed or tested the associated security control or procedure, and/or interviewed the responsible agency officials to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve the underlying control deficiency. Based on this assessment and CDC status reports, we defined the status of each recommendation into the following 3 categories:

- **closed-implemented**—CDC had implemented the recommendation;
- **open-partially implemented**—CDC had made progress toward, but had not completed, implementing the recommendation; and
- **open-not implemented**—CDC had not provided evidence that it had acted to implement the recommendation.

We conducted this performance audit from December 2016 to December 2018 in accordance with generally accepted government auditing

[12] GAO-18-437SU.

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: The National Institute of Standards and Technology 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, as described in the table.

Table 4: National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity

Category	Subcategory
Identify (ID) core 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 organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.
Identify (ID) core 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 organizational objectives and the organization's risk strategy.	ID.AM-2: Software platforms and applications within the organization are inventoried.

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 organizational objectives and the organization's risk strategy.

[1] 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 the prior administration, *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.

Category	Subcategory
Identify (ID) core 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 organizational objectives and the organization’s risk strategy.	ID.AM-3: Organizational communication and data flows are mapped.
Identify (ID) core 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 organizational objectives and the organization’s risk strategy.	ID.AM-4: External information systems are catalogued.
Identify (ID) core 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 organizational objectives and the organization’s risk strategy.	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
Identify (ID) core 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 organizational objectives and the organization’s risk strategy.	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.
Identify (ID) core function: 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.
Identify (ID) core function: 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-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated.
Identify (ID) core function: 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-3: Priorities for organizational mission, objectives, and activities are established and communicated.

Category	Subcategory
Identify (ID) core function: 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-4: Dependencies and critical functions for delivery of critical services are established.
Identify (ID) core function: 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-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational cybersecurity policy is established and communicated.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, 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.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-4: Governance and risk management processes address cybersecurity risks.
Identify (ID) core function: 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.

Category	Subcategory
Identify (ID) core function: 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-2: Cyber threat intelligence is received from information sharing forums and sources.
Identify (ID) core function: 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-3: Threats, both internal and external, are identified and documented.
Identify (ID) core function: 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-4: Potential business impacts and likelihoods are identified.
Identify (ID) core function: 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-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Identify (ID) core function: 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-6: Risk responses are identified and prioritized.
Identify (ID) core function: 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.
Identify (ID) core function: 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-2: Organizational risk tolerance is determined and clearly expressed.
Identify (ID) core function: 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-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Category	Subcategory
Identify (ID) core function: 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.
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.
Protect (PR) core 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.

Category	Subcategory
Protect (PR) core 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-2: Physical access to assets is managed and protected.
Protect (PR) core 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-3: Remote access is managed.
Protect (PR) core 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-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
Protect (PR) core 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-5: Network integrity is protected (e.g., network segregation and network segmentation).
Protect (PR) core 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-6: Identities are proofed and bound to credentials and asserted in interactions.
Protect (PR) core 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-7: Users, devices, and other assets are authenticated (e.g., single-factor and multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Category	Subcategory
Protect (PR) core function: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained.
Protect (PR) core function: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-2: Privileged users understand their roles and responsibilities.
Protect (PR) core function: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
Protect (PR) core function: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-4: Senior executives understand their roles and responsibilities.
Protect (PR) core function: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.
Protect (PR) core function: 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.
Protect (PR) core function: 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-2: Data-in-transit is protected.
Protect (PR) core function: 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-3: Assets are formally managed throughout removal, transfers, and disposition.

Category	Subcategory
Protect (PR) core function: 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-4: Adequate capacity to ensure availability is maintained.
Protect (PR) core function: 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-5: Protections against data leaks are implemented.
Protect (PR) core function: 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-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
Protect (PR) core function: 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-7: The development and testing environment(s) are separate from the production environment.
Protect (PR) core function: 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-8: Integrity checking mechanisms are used to verify hardware integrity.
Protect (PR) core function: 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).
Protect (PR) core function: 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-2: A System Development Life Cycle to manage systems is implemented.
Protect (PR) core function: 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-3: Configuration change control processes are in place.

Category	Subcategory
Protect (PR) core function: 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-4: Backups of information are conducted, maintained, and tested.
Protect (PR) core function: 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-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
Protect (PR) core function: 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-6: Data are destroyed according to policy.
Protect (PR) core function: 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-7: Protection processes are improved.
Protect (PR) core function: 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-8: Effectiveness of protection technologies is shared.
Protect (PR) core function: 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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

Category	Subcategory
Protect (PR) core function: 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-10: Response and recovery plans are tested.
Protect (PR) core function: 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-11: Cybersecurity is included in human resources practices (e.g., deprovisioning and personnel screening).
Protect (PR) core function: 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-12: A vulnerability management plan is developed and implemented **Protect (PR) core function:**.
Protect (PR) core function: Protect (PR) core function: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
Protect (PR) core function: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
Prot Protect (PR) core function: ective 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.
Protect (PR) core function: 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-2: Removable media is protected and its use restricted according to policy.

Category	Subcategory
Protect (PR) core function: 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-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
Protect (PR) core function: 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-4: Communications and control networks are protected.
Protect (PR) core function: 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-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
Detect (DE) core 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.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-4: Impact of events is determined.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-5: Incident alert thresholds are established.
Detect (DE) core function: 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.
Detect (DE) core function: 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-2: The physical environment is monitored to detect potential cybersecurity events.
Detect (DE) core function: 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-3: Personnel activity is monitored to detect potential cybersecurity events.

Category	Subcategory
Detect (DE) core function: 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-4: Malicious code is detected.
Detect (DE) core function: 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-5: Unauthorized mobile code is detected.
Detect (DE) core function: 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-6: External service provider activity is monitored to detect potential cybersecurity events.
Detect (DE) core function: 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-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
Detect (DE) core function: 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-8: Vulnerability scans are performed.
Detect (DE) core function: 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.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-2: Detection activities comply with all applicable requirements.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-3: Detection processes are tested.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4: Event detection information is communicated.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-5: Detection processes are continuously improved.

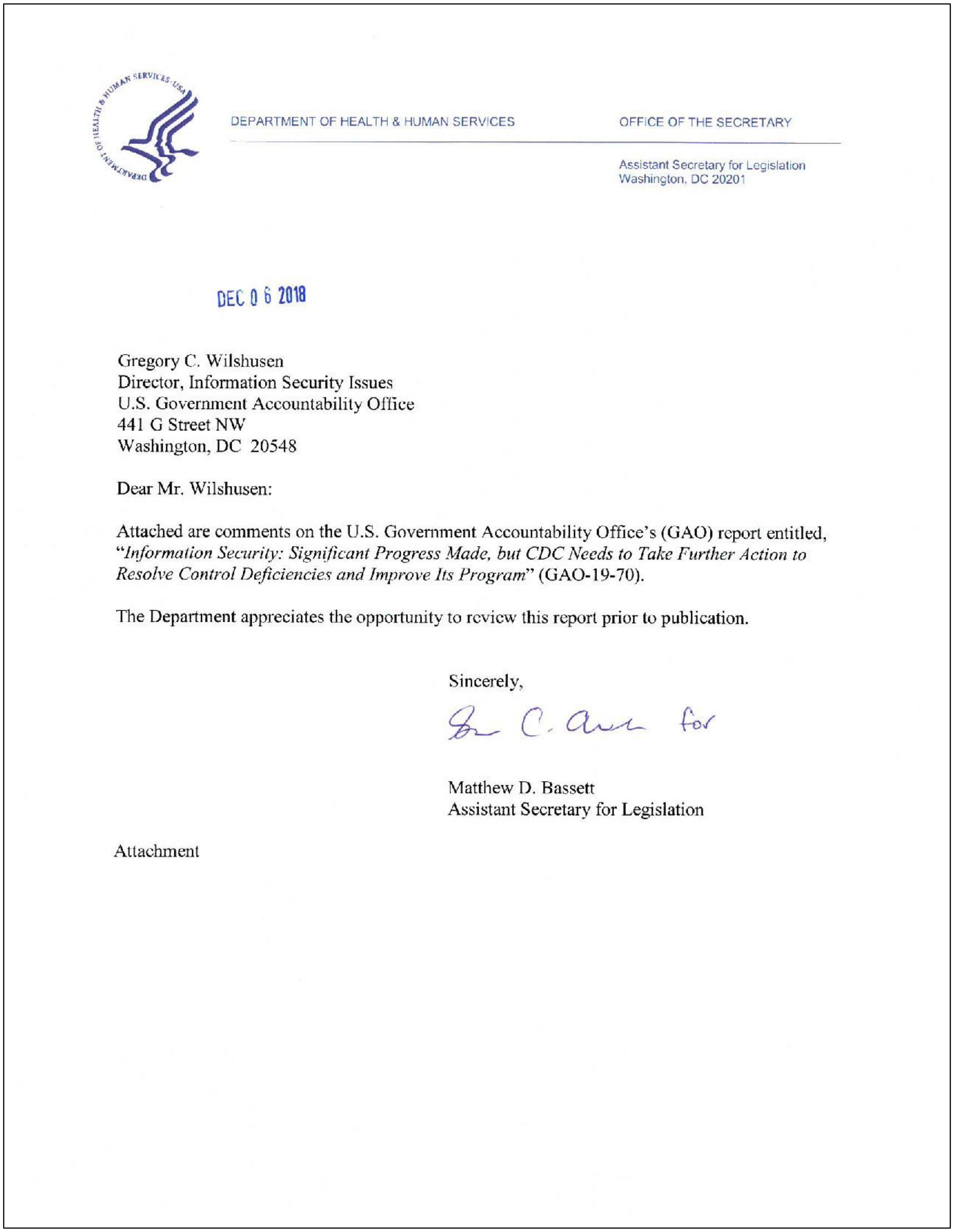
Category	Subcategory
Respond (RS) core function: Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-2: Incidents are reported consistent with established criteria.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-3: Information is shared consistent with response plans.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-2: The impact of the incident is understood.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-3: Forensics are performed.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-4: Incidents are categorized consistent with response plans.

Category	Subcategory
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	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).
Respond (RS) core function: 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.
Respond (RS) core function: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-2: Incidents are mitigated.
Respond (RS) core function: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
Respond (RS) core function: 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.
Respond (RS) core function: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-2: Response strategies are updated.
Recover (RC) core function: Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.
Recover (RC) core function: Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.
Recover (RC) core function: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RC.IM-2: Recovery strategies are updated.
Recover (RC) core function: Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed.

Category	Subcategory
Recover (RC) core function: Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-2: Reputation is repaired after an incident.
Recover (RC) core function: Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	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-19-70

Appendix III: Comments from Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

DEC 0 6 2018

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Information Security: Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program*" (GAO-19-70).

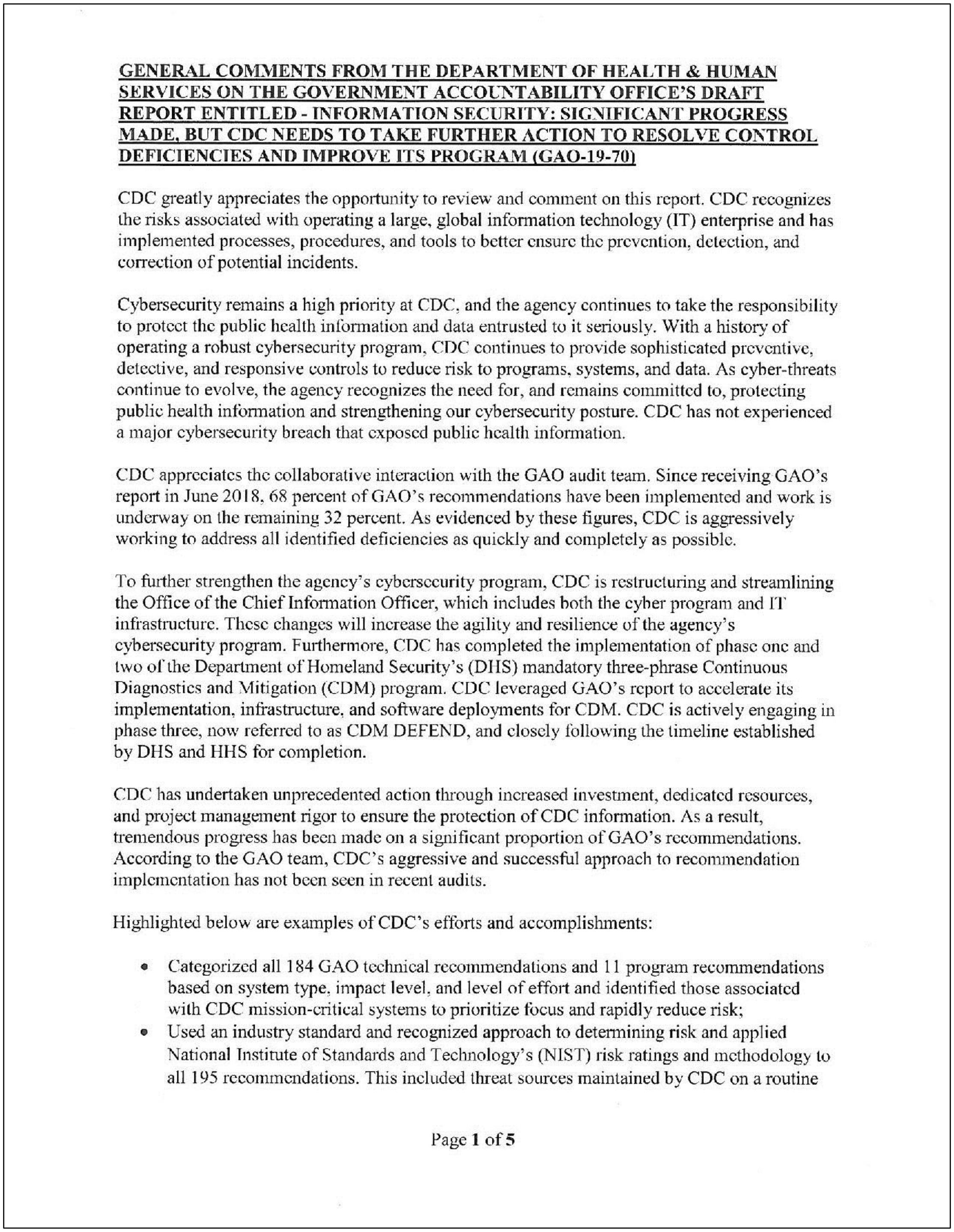
The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

for

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - INFORMATION SECURITY: SIGNIFICANT PROGRESS MADE, BUT CDC NEEDS TO TAKE FURTHER ACTION TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM (GAO-19-70)

CDC greatly appreciates the opportunity to review and comment on this report. CDC recognizes the risks associated with operating a large, global information technology (IT) enterprise and has implemented processes, procedures, and tools to better ensure the prevention, detection, and correction of potential incidents.

Cybersecurity remains a high priority at CDC, and the agency continues to take the responsibility to protect the public health information and data entrusted to it seriously. With a history of operating a robust cybersecurity program, CDC continues to provide sophisticated preventive, detective, and responsive controls to reduce risk to programs, systems, and data. As cyber-threats continue to evolve, the agency recognizes the need for, and remains committed to, protecting public health information and strengthening our cybersecurity posture. CDC has not experienced a major cybersecurity breach that exposed public health information.

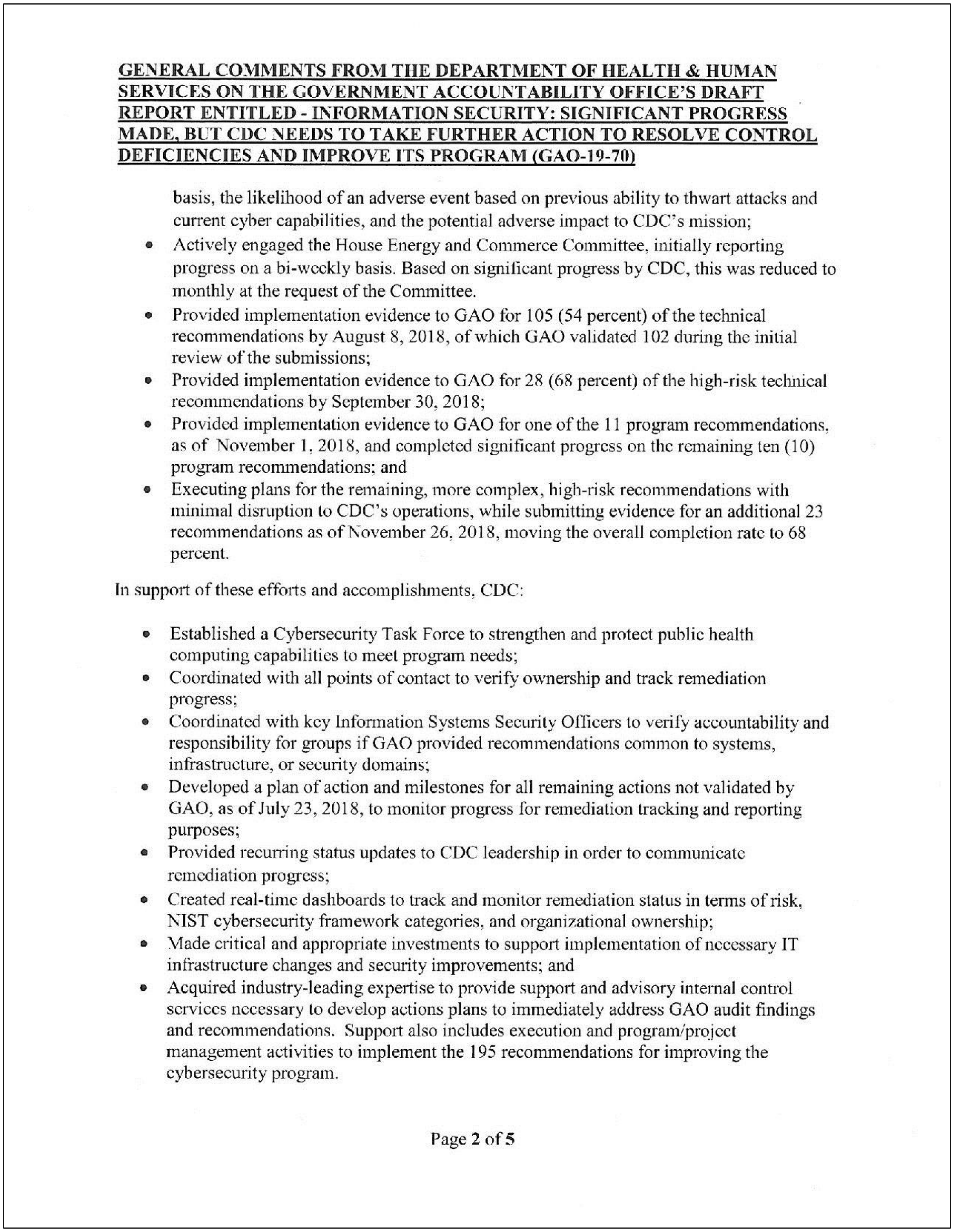
CDC appreciates the collaborative interaction with the GAO audit team. Since receiving GAO's report in June 2018, 68 percent of GAO's recommendations have been implemented and work is underway on the remaining 32 percent. As evidenced by these figures, CDC is aggressively working to address all identified deficiencies as quickly and completely as possible.

To further strengthen the agency's cybersecurity program, CDC is restructuring and streamlining the Office of the Chief Information Officer, which includes both the cyber program and IT infrastructure. These changes will increase the agility and resilience of the agency's cybersecurity program. Furthermore, CDC has completed the implementation of phase one and two of the Department of Homeland Security's (DHS) mandatory three-phrase Continuous Diagnostics and Mitigation (CDM) program. CDC leveraged GAO's report to accelerate its implementation, infrastructure, and software deployments for CDM. CDC is actively engaging in phase three, now referred to as CDM DEFEND, and closely following the timeline established by DHS and HHS for completion.

CDC has undertaken unprecedented action through increased investment, dedicated resources, and project management rigor to ensure the protection of CDC information. As a result, tremendous progress has been made on a significant proportion of GAO's recommendations. According to the GAO team, CDC's aggressive and successful approach to recommendation implementation has not been seen in recent audits.

Highlighted below are examples of CDC's efforts and accomplishments:

- Categorized all 184 GAO technical recommendations and 11 program recommendations based on system type, impact level, and level of effort and identified those associated with CDC mission-critical systems to prioritize focus and rapidly reduce risk;
- Used an industry standard and recognized approach to determining risk and applied National Institute of Standards and Technology's (NIST) risk ratings and methodology to all 195 recommendations. This included threat sources maintained by CDC on a routine



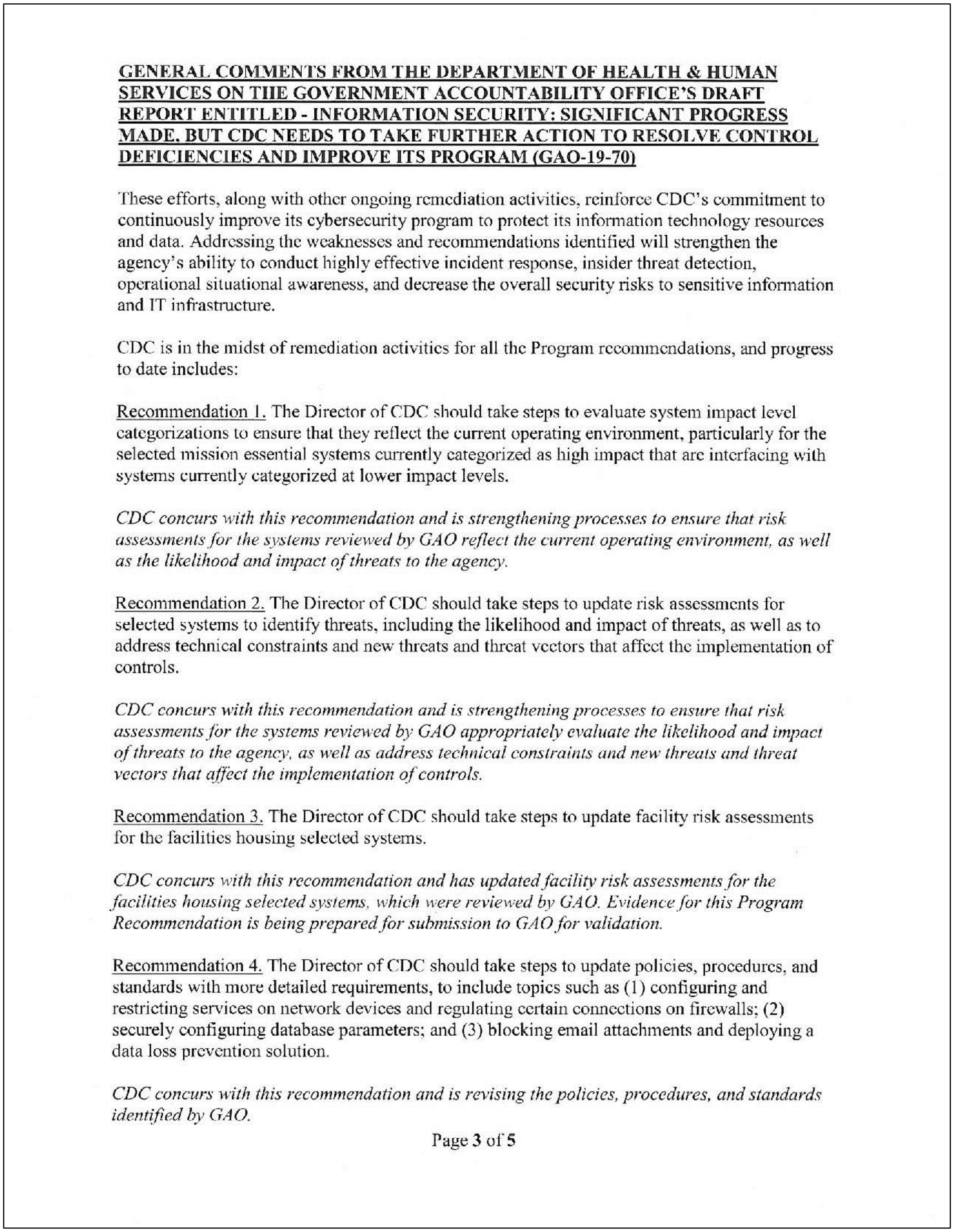
GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - INFORMATION SECURITY: SIGNIFICANT PROGRESS MADE, BUT CDC NEEDS TO TAKE FURTHER ACTION TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM (GAO-19-70)

basis, the likelihood of an adverse event based on previous ability to thwart attacks and current cyber capabilities, and the potential adverse impact to CDC's mission;

- Actively engaged the House Energy and Commerce Committee, initially reporting progress on a bi-weekly basis. Based on significant progress by CDC, this was reduced to monthly at the request of the Committee.
- Provided implementation evidence to GAO for 105 (54 percent) of the technical recommendations by August 8, 2018, of which GAO validated 102 during the initial review of the submissions;
- Provided implementation evidence to GAO for 28 (68 percent) of the high-risk technical recommendations by September 30, 2018;
- Provided implementation evidence to GAO for one of the 11 program recommendations, as of November 1, 2018, and completed significant progress on the remaining ten (10) program recommendations; and
- Executing plans for the remaining, more complex, high-risk recommendations with minimal disruption to CDC's operations, while submitting evidence for an additional 23 recommendations as of November 26, 2018, moving the overall completion rate to 68 percent.

In support of these efforts and accomplishments, CDC:

- Established a Cybersecurity Task Force to strengthen and protect public health computing capabilities to meet program needs;
- Coordinated with all points of contact to verify ownership and track remediation progress;
- Coordinated with key Information Systems Security Officers to verify accountability and responsibility for groups if GAO provided recommendations common to systems, infrastructure, or security domains;
- Developed a plan of action and milestones for all remaining actions not validated by GAO, as of July 23, 2018, to monitor progress for remediation tracking and reporting purposes;
- Provided recurring status updates to CDC leadership in order to communicate remediation progress;
- Created real-time dashboards to track and monitor remediation status in terms of risk, NIST cybersecurity framework categories, and organizational ownership;
- Made critical and appropriate investments to support implementation of necessary IT infrastructure changes and security improvements; and
- Acquired industry-leading expertise to provide support and advisory internal control services necessary to develop actions plans to immediately address GAO audit findings and recommendations. Support also includes execution and program/project management activities to implement the 195 recommendations for improving the cybersecurity program.



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - INFORMATION SECURITY: SIGNIFICANT PROGRESS MADE, BUT CDC NEEDS TO TAKE FURTHER ACTION TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM (GAO-19-70)

These efforts, along with other ongoing remediation activities, reinforce CDC's commitment to continuously improve its cybersecurity program to protect its information technology resources and data. Addressing the weaknesses and recommendations identified will strengthen the agency's ability to conduct highly effective incident response, insider threat detection, operational situational awareness, and decrease the overall security risks to sensitive information and IT infrastructure.

CDC is in the midst of remediation activities for all the Program recommendations, and progress to date includes:

Recommendation 1. The Director of CDC should take steps to evaluate system impact level categorizations to ensure that they reflect the current operating environment, particularly for the selected mission essential systems currently categorized as high impact that are interfacing with systems currently categorized at lower impact levels.

CDC concurs with this recommendation and is strengthening processes to ensure that risk assessments for the systems reviewed by GAO reflect the current operating environment, as well as the likelihood and impact of threats to the agency.

Recommendation 2. The Director of CDC should take steps to update risk assessments for selected systems to identify threats, including the likelihood and impact of threats, as well as to address technical constraints and new threats and threat vectors that affect the implementation of controls.

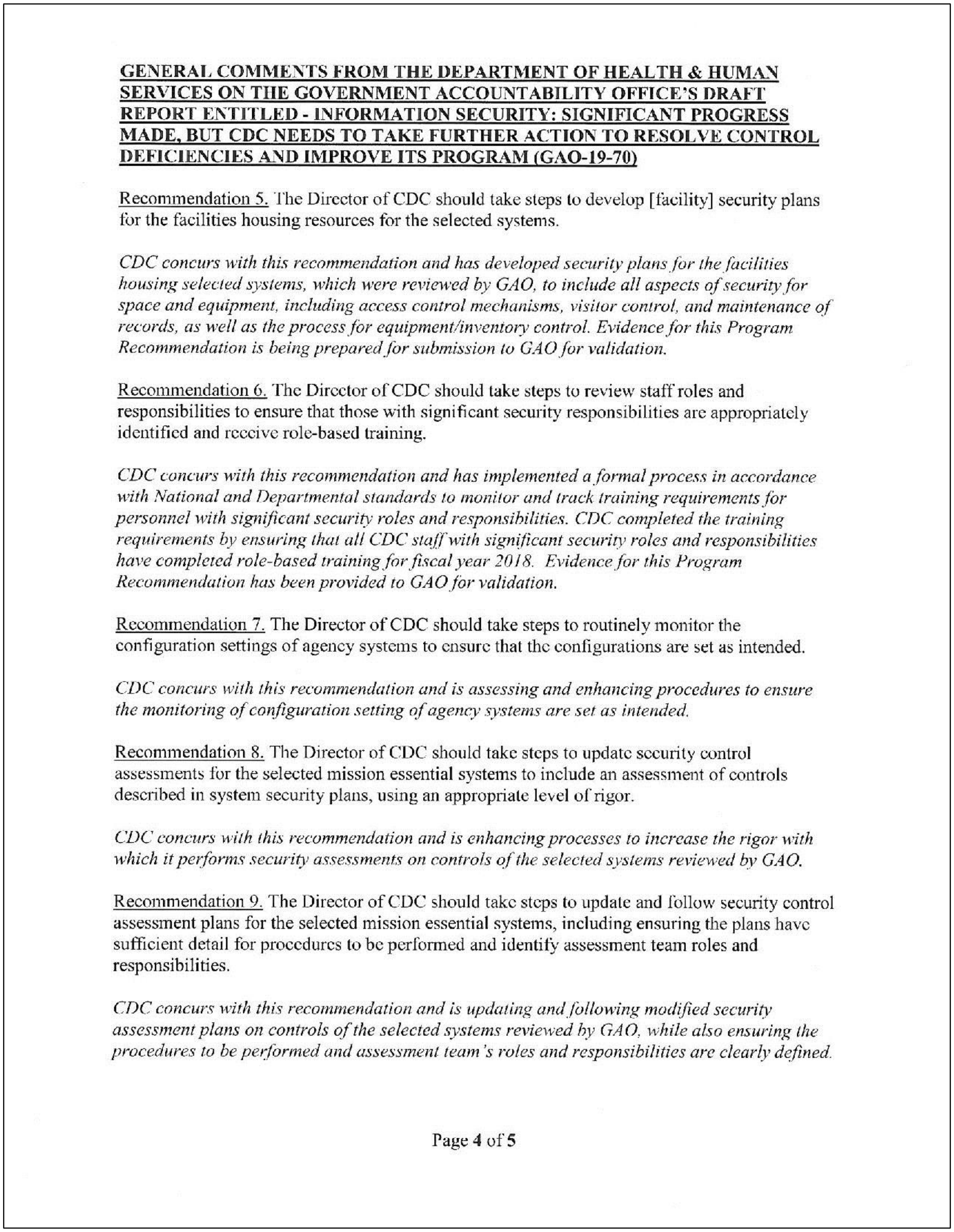
CDC concurs with this recommendation and is strengthening processes to ensure that risk assessments for the systems reviewed by GAO appropriately evaluate the likelihood and impact of threats to the agency, as well as address technical constraints and new threats and threat vectors that affect the implementation of controls.

Recommendation 3. The Director of CDC should take steps to update facility risk assessments for the facilities housing selected systems.

CDC concurs with this recommendation and has updated facility risk assessments for the facilities housing selected systems, which were reviewed by GAO. Evidence for this Program Recommendation is being prepared for submission to GAO for validation.

Recommendation 4. The Director of CDC should take steps to update policies, procedures, and standards with more detailed requirements, to include topics such as (1) configuring and restricting services on network devices and regulating certain connections on firewalls; (2) securely configuring database parameters; and (3) blocking email attachments and deploying a data loss prevention solution.

CDC concurs with this recommendation and is revising the policies, procedures, and standards identified by GAO.



<u>GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - INFORMATION SECURITY: SIGNIFICANT PROGRESS MADE, BUT CDC NEEDS TO TAKE FURTHER ACTION TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM (GAO-19-70)</u>

<u>Recommendation 5.</u> The Director of CDC should take steps to develop [facility] security plans for the facilities housing resources for the selected systems.

CDC concurs with this recommendation and has developed security plans for the facilities housing selected systems, which were reviewed by GAO, to include all aspects of security for space and equipment, including access control mechanisms, visitor control, and maintenance of records, as well as the process for equipment/inventory control. Evidence for this Program Recommendation is being prepared for submission to GAO for validation.

<u>Recommendation 6.</u> The Director of CDC should take steps to review staff roles and responsibilities to ensure that those with significant security responsibilities are appropriately identified and receive role-based training.

CDC concurs with this recommendation and has implemented a formal process in accordance with National and Departmental standards to monitor and track training requirements for personnel with significant security roles and responsibilities. CDC completed the training requirements by ensuring that all CDC staff with significant security roles and responsibilities have completed role-based training for fiscal year 2018. Evidence for this Program Recommendation has been provided to GAO for validation.

<u>Recommendation 7.</u> The Director of CDC should take steps to routinely monitor the configuration settings of agency systems to ensure that the configurations are set as intended.

CDC concurs with this recommendation and is assessing and enhancing procedures to ensure the monitoring of configuration setting of agency systems are set as intended.

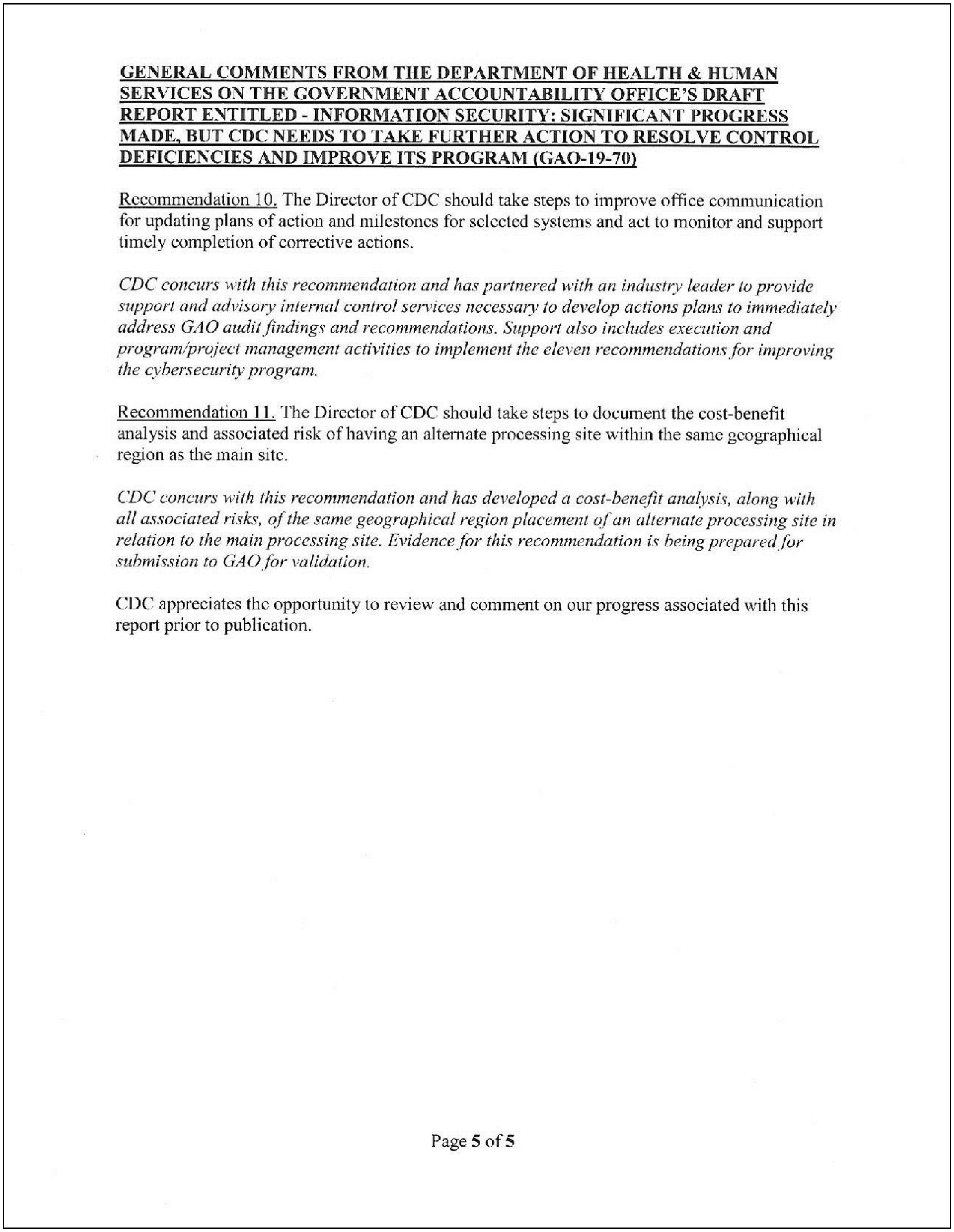
<u>Recommendation 8.</u> The Director of CDC should take steps to update security control assessments for the selected mission essential systems to include an assessment of controls described in system security plans, using an appropriate level of rigor.

CDC concurs with this recommendation and is enhancing processes to increase the rigor with which it performs security assessments on controls of the selected systems reviewed by GAO.

<u>Recommendation 9.</u> The Director of CDC should take steps to update and follow security control assessment plans for the selected mission essential systems, including ensuring the plans have sufficient detail for procedures to be performed and identify assessment team roles and responsibilities.

CDC concurs with this recommendation and is updating and following modified security assessment plans on controls of the selected systems reviewed by GAO, while also ensuring the procedures to be performed and assessment team's roles and responsibilities are clearly defined.

Page **4** of **5**



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - INFORMATION SECURITY: SIGNIFICANT PROGRESS MADE, BUT CDC NEEDS TO TAKE FURTHER ACTION TO RESOLVE CONTROL DEFICIENCIES AND IMPROVE ITS PROGRAM (GAO-19-70)

Recommendation 10. The Director of CDC should take steps to improve office communication for updating plans of action and milestones for selected systems and act to monitor and support timely completion of corrective actions.

CDC concurs with this recommendation and has partnered with an industry leader to provide support and advisory internal control services necessary to develop actions plans to immediately address GAO audit findings and recommendations. Support also includes execution and program/project management activities to implement the eleven recommendations for improving the cybersecurity program.

Recommendation 11. The Director of CDC should take steps to document the cost-benefit analysis and associated risk of having an alternate processing site within the same geographical region as the main site.

CDC concurs with this recommendation and has developed a cost-benefit analysis, along with all associated risks, of the same geographical region placement of an alternate processing site in relation to the main processing site. Evidence for this recommendation is being prepared for submission to GAO for validation.

CDC appreciates the opportunity to review and comment on our progress associated with this report prior to publication.

Page **5** of **5**

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Gary Austin, Jennifer R. Franks, Jeffrey Knott, and Chris Warweg (assistant directors); Chibuikem Ajulu-Okeke, Angela Bell, Sa'ar Dagani, Nancy Glover, Chaz Hubbard, George Kovachick, Sean Mays, Kevin Metcalf, Brandon Sanders, Michael Stevens, Daniel Swartz, and Angela Watson made key contributions to this report. Edward Alexander, Jr. and Duc Ngo (assistant directors); David Blanding, and Christopher Businsky also provided assistance.

Appendix V: Accessible Data

Data Tables

Accessible Data for Status of GAO Recommendations to the Centers for Disease Control and Prevention

Open	No Evidence	Open-Partial
72	21	102

Accessible Data for Figure 1: Methods Used by the Centers for Disease Control and Prevention to Assess Security Controls

Interview and examine	Examine	Interview	Test	Unidentified
52	49	38	37	15

Accessible Data for Figure 2: The Centers for Disease Control and Prevention's Planned Timeline for Fully Implementing GAO's Technical Control-Related Recommendations

Month	Number of open recommendations
Mar-2018	184
Apr-2018	184
May-2018	184
Jun-2018	169
Jun-2018	169
Jul-2018	169
Aug-2018	82
Aug-2018	52
Sep-2018	50
Oct-2018	50
Nov-2018	50
Dec-2018	46
Jan-2019	45
Feb-2019	45
Mar-2019	23
Apr-2019	23

Month	Number of open recommendations
May-2019	23
Jun-2019	14
Jul-2019	14
Jul-2019	14
Aug-2019	11
Sep-2019	5
Oct-2019	5
Nov-2019	5
Dec-2019	5
Jan-2020	5
Feb-2020	5
Mar-2020	2
Apr-2020	2
May-2020	2
Jun-2020	2
Jul-2020	2
Aug-2020	2
Sep-2020	2
Sep-2020	2

Agency Comment Letter

Accessible Text for Appendix III Comments from Department of Health and Human Services

Page 1

DEC 06 2018

Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office

441 G Street NW

Washington, DC 20548

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, “Information Security: Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program” (GAO-19-70).

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

Sincerely,

Matthew D. Bassett

Assistant Secretary for Legislation

Attachment

Page 2

CDC greatly appreciates the opportunity to review and comment on this report. CDC recognizes the risks associated with operating a large, global information technology (IT) enterprise and has implemented processes, procedures, and tools to better ensure the prevention, detection, and correction of potential incidents.

Cybersecurity remains a high priority at CDC, and the agency continues to take the responsibility to protect the public health information and data entrusted to it seriously. With a history of operating a robust cybersecurity program, CDC continues to provide sophisticated preventive, detective, and responsive controls to reduce risk to programs, systems, and data. As cyber-threats continue to evolve, the agency recognizes the need for, and remains committed to, protecting public health information and strengthening our cybersecurity posture. CDC has not experienced a major cybersecurity breach that exposed public health information.

CDC appreciates the collaborative interaction with the GAO audit team. Since receiving GAO's report in June 2018, 68 percent of GAO's recommendations have been implemented and work is underway on the remaining 32 percent. As evidenced by these figures, CDC is aggressively working to address all identified deficiencies as quickly and completely as possible.

To further strengthen the agency's cybersecurity program, CDC is restructuring and streamlining the Office of the Chief Information Officer, which includes both the cyber program and IT infrastructure. These changes will increase the agility and resilience of the agency's cybersecurity program. Furthermore, CDC has completed the implementation of phase one and two of the Department of Homeland Security's (DHS) mandatory three-phrase Continuous Diagnostics and Mitigation (CDM) program. CDC leveraged GAO's report to accelerate its implementation, infrastructure, and software deployments for CDM. CDC is actively engaging in phase three, now referred to as CDM DEFEND, and closely following the timeline established by DHS and HHS for completion.

CDC has undertaken unprecedented action through increased investment, dedicated resources, and project management rigor to ensure the protection of CDC information. As a result, tremendous progress has been made on a significant proportion of GAO's recommendations. According to the GAO team, CDC's aggressive and successful approach to recommendation implementation has not been seen in recent audits.

Highlighted below are examples of CDC's efforts and accomplishments:

- Categorized all 184 GAO technical recommendations and 11 program recommendations based on system type, impact level, and level of effort and identified those associated with CDC mission-critical systems to prioritize focus and rapidly reduce risk;

- Used an industry standard and recognized approach to determining risk and applied National Institute of Standards and Technology's (NIST) risk ratings and methodology to all 195 recommendations. This included threat sources maintained by CDC on a routine

Page 3

basis, the likelihood of an adverse event based on previous ability to thwart attacks and current cyber capabilities, and the potential adverse impact to CDC's mission;

- Actively engaged the House Energy and Commerce Committee, initially reporting progress on a bi-weekly basis. Based on significant progress by CDC, this was reduced to monthly at the request of the Committee.

- Provided implementation evidence to GAO for 105 (54 percent) of the technical recommendations by August 8, 2018, of which GAO validated 102 during the initial review of the submissions;

- Provided implementation evidence to GAO for 28 (68 percent) of the high-risk technical recommendations by September 30, 2018;

- Provided implementation evidence to GAO for one of the 11 program recommendations, as of November 1, 2018, and completed significant progress on the remaining ten (10) program recommendations; and

- Executing plans for the remaining, more complex, high-risk recommendations with minimal disruption to CDC's operations, while submitting evidence for an additional 23 recommendations as of November 26, 2018, moving the overall completion rate to 68 percent.

In support of these efforts and accomplishments, CDC:

- Established a Cybersecurity Task Force to strengthen and protect public health computing capabilities to meet program needs;

- Coordinated with all points of contact to verify ownership and track remediation progress;

- Coordinated with key Information Systems Security Officers to verify accountability and responsibility for groups if GAO provided recommendations common to systems, infrastructure, or security domains;

- Developed a plan of action and milestones for all remaining actions not validated by GAO, as of July 23, 2018, to monitor progress for remediation tracking and reporting purposes;

- Provided recurring status updates to CDC leadership in order to communicate remediation progress;

- Created real-time dashboards to track and monitor remediation status in terms of risk, NIST cybersecurity framework categories, and organizational ownership;
- Made critical and appropriate investments to support implementation of necessary IT infrastructure changes and security improvements; and
- Acquired industry-leading expertise to provide support and advisory internal control services necessary to develop actions plans to immediately address GAO audit findings and recommendations. Support also includes execution and program/project management activities to implement the 195 recommendations for improving the cybersecurity program.

Page 4

These efforts, along with other ongoing remediation activities, reinforce CDC's commitment to continuously improve its cybersecurity program to protect its information technology resources and data. Addressing the weaknesses and recommendations identified will strengthen the agency's ability to conduct highly effective incident response, insider threat detection, operational situational awareness, and decrease the overall security risks to sensitive information and IT infrastructure.

CDC is in the midst of remediation activities for all the Program recommendations, and progress to date includes:

Recommendation 1. The Director of CDC should take steps to evaluate system impact level categorizations to ensure that they reflect the current operating environment, particularly for the selected mission essential systems currently categorized as high impact that are interfacing with systems currently categorized at lower impact levels.

CDC concurs with this recommendation and is strengthening processes to ensure that risk assessments for the systems reviewed by GAO reflect the current operating environment, as well as the likelihood and impact of threats to the agency.

Recommendation 2. The Director of CDC should take steps to update risk assessments for selected systems to identify threats, including the likelihood and impact of threats, as well as to address technical constraints and new threats and threat vectors that affect the implementation of controls.

CDC concurs with this recommendation and is strengthening processes to ensure that risk assessments for the systems reviewed by GAO appropriately evaluate the likelihood and impact of threats to the agency, as well as address technical constraints and new threats and threat vectors that affect the implementation of controls.

Recommendation 3. The Director of CDC should take steps to update facility risk assessments for the facilities housing selected systems.

CDC concurs with this recommendation and has updated facility risk assessments for the facilities housing selected systems, which were reviewed by GAO. Evidence for this Program Recommendation is being prepared for submission to GAO for validation.

Recommendation 4. The Director of CDC should take steps to update policies, procedures, and standards with more detailed requirements, to include topics such as (1) configuring and restricting services on network devices and regulating certain connections on firewalls; (2) securely configuring database parameters; and (3) blocking email attachments and deploying a data loss prevention solution.

CDC concurs with this recommendation and is revising the policies, procedures, and standards identified by GAO.

Page 5

Recommendation 5. The Director of CDC should take steps to develop [facility] security plans for the facilities housing resources for the selected systems.

CDC concurs with this recommendation and has developed security plans for the facilities housing selected systems, which were reviewed by GAO, to include all aspects of security for space and equipment, including access control mechanisms, visitor control, and maintenance of records, as well as the process for equipment/inventory control. Evidence for this Program Recommendation is being prepared for submission to GAO for validation.

Recommendation 6. The Director of CDC should take steps to review staff roles and responsibilities to ensure that those with significant security responsibilities are appropriately identified and receive role-based training.

CDC concurs with this recommendation and has implemented a formal process in accordance with National and Departmental standards to monitor and track training requirements for personnel with significant security roles and responsibilities. CDC completed the training requirements by ensuring that all CDC staff with significant security roles and responsibilities have completed role-based training for fiscal year 2018. Evidence for this Program Recommendation has been provided to GAO for validation.

Recommendation 7. The Director of CDC should take steps to routinely monitor the configuration settings of agency systems to ensure that the configurations are set as intended.

CDC concurs with this recommendation and is assessing and enhancing procedures to ensure the monitoring of configuration setting of agency systems are set as intended.

Recommendation 8. The Director of CDC should take steps to update security control assessments for the selected mission essential systems to include an assessment of controls described in system security plans, using an appropriate level of rigor.

CDC concurs with this recommendation and is enhancing processes to increase the rigor with which it performs security assessments on controls of the selected systems reviewed by GAO.

Recommendation 9. The Director of CDC should take steps to update and follow security control assessment plans for the selected mission essential systems, including ensuring the plans have sufficient detail for procedures to be performed and identify assessment team roles and responsibilities.

CDC concurs with this recommendation and is updating and following modified security assessment plans on controls of the selected systems reviewed by GAO, while also ensuring the procedures to be performed and assessment team's roles and responsibilities are clearly defined.

Page 6

Recommendation 10. The Director of CDC should take steps to improve office communication for updating plans of action and milestones for selected systems and act to monitor and support timely completion of corrective actions.

CDC concurs with this recommendation and has partnered with an industry leader to provide support and advisory internal control sen1ices necessary to develop actions plans to immediately address GAO audit findings and recommendations. Support also includes execution and program/project management activities to implement the eleven recommendations for improving the cybersecurity program.

Recommendation 11. The Director of CDC should take steps to document the cost-benefit analysis and associated risk of having an alternate processing site within the same geographical region as the main site.

CDC concurs with this recommendation and has developed a cost-benefit analysis, along with all associated risks, of the same geographical region placement of an alternate processing site in relation to the main processing site. Evidence for this recommendation is being prepared for submission to GAO for validation.

CDC appreciates the opportunity to review and comment on our progress associated with this report prior to publication.

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

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