United States Government Accountability Office

Report to Congressional Requesters

March 2021

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation

Accessible Version

A Century of Non-Partisan Fact-Based Work

GAO-21-236

GAO Highlights

Highlights of GAO-21-236, a report to congressional requesters

March 2021

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation

Why GAO Did This Study

Threats to the nation's critical infrastructures and the information technology systems that support them require a concerted effort among federal agencies; state, local, tribal, and territorial governments; and the private sector to ensure their security. The seriousness of the threat was reinforced by the December 2020 discovery of a cyberattack that has had widespread impact on government agencies, critical infrastructures, and private-sector companies.

Federal legislation enacted in November 2018 established CISA to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.

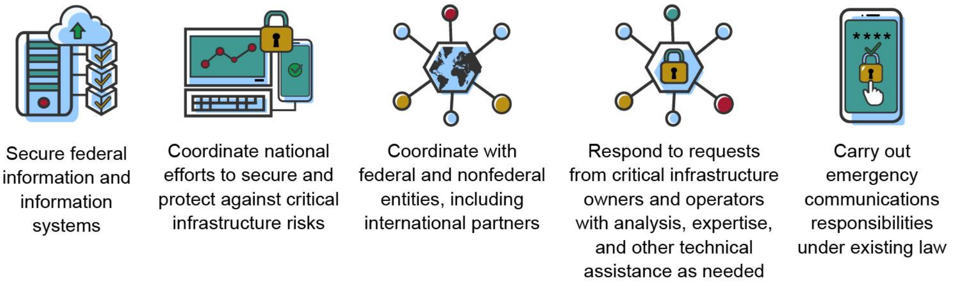
GAO was asked to review CISA's organizational transformative initiative and its ability to coordinate effectively with stakeholders. The objectives of GAO's review were to (1) describe CISA's organizational transformation initiative, (2) assess the current progress of the initiative, (3) determine the extent to which CISA's transformation efforts align with key practices for effective agency reform, and (4) identify any challenges in CISA's coordination with stakeholders, and assess strategies the agency has developed to address such challenges.

View GAO-21-236. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Nathan Anderson at (206) 287-4804 or andersonn@gao.gov.

What GAO Found

To implement the requirements of the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018, CISA leadership within the Department of Homeland Security launched an organizational transformation initiative. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency. (See figure 1 below.) CISA completed the first two of three phases of its organizational transformation initiative, which resulted in, among other things, a new organization chart, consolidation of multiple incident response centers, and consolidation of points of contact for infrastructure security stakeholders. Phase three is intended to fully implement the agency's planned organizational changes.

Figure 1: Five Key Responsibilities Assigned to the Cybersecurity and Infrastructure Security Agency (CISA)


Secure federal information and information systems
Coordinate national efforts to secure and protect against critical infrastructure risks
Coordinate with federal and nonfederal entities, including international partners
Respond to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance as needed
Carry out emergency communications responsibilities under existing law

Source: GAO analysis of the CISA Act of 2018; images: Buffaloboy/stock.adobe.com. | GAO-21-236

Text of Figure 1: Five Key Responsibilities Assigned to the Cybersecurity and Infrastructure Security Agency (CISA)

1. Secure federal information and information systems
2. Coordinate national efforts to secure and protect against critical infrastructure risks
3. Coordinate with federal and nonfederal entities, including international partners
4. Respond to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance as needed
5. Carry out emergency communications responsibilities under existing law

Source: GAO analysis of the CISA Act of 2018. | GAO-21-236

While CISA intended to fully implement the transformation by December 2020, it had completed 37 of 94 planned tasks for phase three by mid-February 2021. Among the tasks not yet completed, 42 of them were past their most recent planned completion dates. Included in these 42 are the tasks of finalizing the

To do this, GAO reviewed relevant information on CISA's efforts to develop an organizational transformation initiative to meet the requirements of the CISA Act of 2018. To assess the progress of CISA's efforts, GAO analyzed agency documentation to determine the status of activities related to the three phases of the organizational transformation and reasons for any delays in its progress. GAO also assessed CISA's efforts against selected key practices identified by GAO that can contribute to the effectiveness of agency reform efforts. In addition, GAO interviewed selected stakeholders related to CISA's primary mission areas to identify any pertinent challenges and analyzed strategies CISA developed to address these challenges.

What GAO Recommends

GAO is making 11 recommendations to CISA:

- Establish new expected completion dates for the phase three tasks that are past their completion dates, with priority given to tasks critical to mission effectiveness.
- Establish an overall deadline for the completion of the transformation initiative.
- Fully address each of the six reform practices that have been either partially or not addressed.
- Develop strategies to mitigate each of the three infrastructure challenges that remain outstanding.

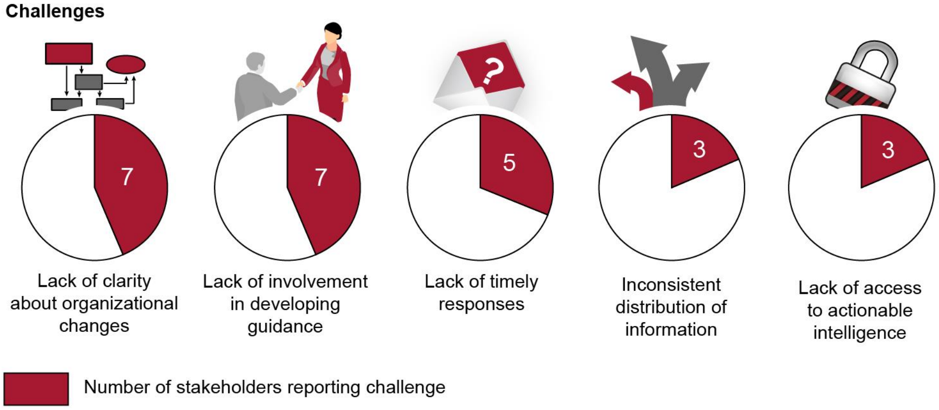
The Department of Homeland Security agreed with GAO's recommendations.

mission-essential functions of CISA's divisions and issuing a memorandum defining incident management roles and responsibilities across CISA. Tasks such as these appear to be critical to CISA's transformation initiative and accordingly its ability to effectively and efficiently carry out its cyber protection mission. In addition, the agency had not established an updated overall deadline for completing its transformation initiative. Until it establishes updated milestones and an overall deadline for its efforts, and expeditiously carries out these plans, CISA will be hindered in meeting the goals of its organizational transformation initiative. This in turn may impair the agency's ability to identify and respond to incidents, such as the cyberattack discovered in December 2020 that caused widespread damage.

Of 10 selected key practices for effective agency reforms previously identified by GAO, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. For example, CISA generally addressed practices related to using data and evidence to support its planned reforms and engaging its employees in the organizational change process. The agency partially addressed practices related to, for example, defining goals and outcomes and conducting workforce planning. Workforce planning is especially important for CISA, given the criticality of hiring and retaining experts who, among other things, can help identify and respond to complex attacks. CISA did conduct an initial assessment of its cybersecurity workforce in 2019; however, it is still working on analyzing capability gaps and determining how to best fill those gaps. Finally, CISA did not address the practice of ensuring that its employee performance management system was aligned with its new organizational structure and transformation goals. Until it fully addresses workforce planning and the five other practices that are either partially or not addressed, CISA's ability to leverage its organizational changes to effectively carry out its mission will be hindered.

Selected government and private-sector stakeholders from the 16 sectors considered to be critical infrastructures, such as banking and financial institutions, telecommunications, and energy, reported a number of challenges in coordinating with CISA. (See figure 2.)

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



Source: GAO analysis of stakeholder interviews. | GAO-21-236

Text of Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors

Challenges

- Lack of clarity about organizational changes reported by 7 stakeholders
- Lack of involvement in developing guidance reported by 7 stakeholders
- Lack of timely response reported by 5 stakeholders
- Inconsistent distribution of information reported by 3 stakeholders.
- Lack of access to actionable intelligence reported by 3 stakeholders.

Source: GAO analysis of stakeholder interviews. | GAO-21-236

CISA has activities under way to mitigate some of these challenges, including tracking stakeholder inquiries to monitor the timeliness of responses and delivering briefings with intelligence tailored to stakeholder needs. However, it has not developed strategies to clarify changes to its organizational structure, have consistent stakeholder involvement in the development of guidance, and distribute information to all key stakeholders. Organizational structure and information distribution are both considered new challenges associated with the reorganization of CISA. Developing strategies to mitigate these challenges could help provide CISA with assurance that its stakeholders are receiving the information and support needed to make decisions about risks facing the nation’s critical infrastructures.

Contents

Tables

Figures

Abbreviations

5G	fifth-generation (wireless networks)
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FPS	Federal Protective Service
GCC	government coordinating council
HSPD	Homeland Security Presidential Directive
IT	information technology
NCC	National Coordinating Center for Communications
NCCIC	National Cybersecurity and Communications Integration Center
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
OMB	Office of Management and Budget
OBIM	Office of Biometric Identity Management
PPD-21	Presidential Policy Directive 21
SCC	sector coordinating council
SSA	sector-specific agency
SWIC	Statewide Interoperability Coordinator

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work
441 G St. N.W.
Washington, DC 20548

March 10, 2021

Congressional Requesters

The nation's critical infrastructures, both physical and cyber, are vulnerable to a wide variety of threats. In addition, the risks to information technology (IT) systems supporting the federal government and the nation's critical infrastructures are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. Because most of the critical infrastructures are owned by the private sector, it is vital that the public and private sectors work together to protect these assets.

The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 established CISA as an operational component agency within the Department of Homeland Security (DHS).[1] The act assigned CISA the responsibility to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats.

Since its establishment, CISA has been reorganizing offices and functions previously organized under the department's National Protection and Programs Directorate (NPPD) and aligning its new organizational structure with its mission. One of CISA's primary responsibilities is coordination with other government and private-sector partners. As the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts, CISA's ability to effectively coordinate and consult with its partners—which include other federal agencies; state, local, territorial, and tribal governments; and the private sector—is critical.

You asked us to review CISA's efforts to establish and implement its organizational transformative initiative and its ability to coordinate effectively with stakeholders. Our specific objectives were to (1) describe CISA's organizational transformation initiative; (2) assess the progress of CISA's organizational transformation initiative, as well as any impact of the Coronavirus Disease 2019 (COVID-19) pandemic on these efforts; (3) determine the extent to which CISA's organizational transformation efforts

[1] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169, section 2202(a)(1) (codified at 6 U.S.C. section 652).

align with key practices for effective agency reforms, including organizational transformations; and (4) identify challenges, if any, that exist in CISA's efforts to coordinate with government and private-sector stakeholders, and strategies the agency has developed to address these challenges.

To address the first objective, we reviewed requirements of the CISA Act of 2018 and other relevant laws, such as the Homeland Security Act of 2002, to identify the agency's key statutory responsibilities. We also reviewed relevant information on CISA leadership's efforts to develop its organizational transformation initiative to implement necessary changes to the agency. In addition, we interviewed CISA's Deputy Director, Chief of Transformation, and other relevant officials to better understand the transformation efforts.[2]

To address the second objective, we reviewed and analyzed relevant information on CISA leadership's efforts to implement its organizational transformation initiative and vision for the agency, including preliminary organization charts, the agency's implementation task list, and associated documentation of tasks completed to date. In addition, we interviewed CISA's Deputy Director, Chief of Transformation, and other relevant officials. We discussed with these officials the reasons for any delays in implementing the organizational transformation and any impact that the COVID-19 pandemic has had on their efforts.

To address the third objective, we selected 10 relevant key practices for assessing agency reforms that we identified in our prior work on federal government reorganization efforts.[3] With respect to these practices, reforms broadly include any organizational changes—such as major transformations, mergers, consolidations, and other reorganizations—and

[2] In November 2020, the Director and Deputy Director of CISA both left the agency. In addition, the official designated as Chief of Transformation had moved to a different division within the agency. According to CISA officials, as of January 2021, the organizational transformation was being overseen by the Acting Deputy Director and the Senior Advisor for the CISA 2020 Transformation.

[3] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018). Reforming and reorganizing the federal government is a major endeavor that can include refocusing, realigning, or enhancing agency missions, as well as taking steps to improve services by identifying and eliminating inefficiencies. Equally important is maintaining or improving effectiveness and examining the impact of such proposed changes on employees, stakeholders, and program customers. Of 12 key practice subcategories identified by GAO, we excluded two because we determined that they were not applicable to CISA's organizational transformation efforts.

efforts to streamline and improve the efficiency and effectiveness of government operations.

We compared the selected practices to information collected from CISA regarding its organizational transformation initiative, including its implementation plan and other documentation, as well as interviews with relevant agency officials. We relied on this analysis to assess the extent to which the agency's efforts addressed each of the selected key practices. Specifically, we determined that the agency's efforts generally addressed the practice if we did not identify significant gaps in its coverage of the actions associated with this practice, partially addressed the practice if we identified significant gaps in its coverage of the actions associated with this practice, and did not address the practice if it had not substantively addressed any of the actions associated with the practice.

To address the fourth objective, we interviewed selected CISA stakeholders associated with the agency's infrastructure protection, cybersecurity, and emergency communication missions. These stakeholders included representatives of the 16 critical infrastructure sectors (eight government coordinating councils (GCC)[4] and eight sector coordinating councils (SCC)),[5] six members of the Federal Chief Information Officers (CIO) Council,[6] three Statewide Interoperability Coordinators (SWIC),[7] and three public safety associations with emergency communications responsibilities.[8] We selected the critical infrastructure stakeholders to ensure that we would get perspectives from

[4] SCCs are self-organized, self-run, and self-governed private-sector councils consisting of owners and operators and their representatives, which interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private-sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities.

[5] GCCs are formed as the government counterpart to the SCC to enable interagency and cross-jurisdictional coordination. Each GCC consists of representatives across various levels of government (federal, state, local, tribal, and territorial), as appropriate to the operating landscape of each sector.

[6] The Chief Information Officers Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal information resources.

[7] SWICs are state-level entities responsible for implementing a statewide strategic vision for emergency communications interoperability.

[8] These three associations were the American Public Works Association, International Association of the Chiefs of Police, and the International Association of Fire Chiefs.

both government and industry/private-sector stakeholders, federal CIOs who would be positioned to answer questions on behalf of the federal CIO council about coordination with CISA, and emergency communications stakeholders based on prior GAO work.

We conducted semi-structured interviews with these stakeholders to understand their relationships with CISA and identify any challenges they experienced in coordinating with CISA, both before and since its reorganization. We also asked these stakeholders about their experiences working with CISA during the COVID-19 pandemic. We then asked CISA about any mitigation strategies that were planned or under way to address these challenges, and collected and analyzed documentation related to these strategies. (See appendix I for additional details on our objectives, scope, and methodology.)

We conducted this performance audit from September 2019 to March 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Our nation’s critical infrastructures consist of systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on the nation’s security, economic stability, public health or safety, or any combination of these factors. Critical infrastructure includes, among other things, banking and financing institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned and operated by the private sector.

Under federal policy, critical infrastructure is grouped into 16 sectors whose assets, systems, and networks, are considered vital to the security, economy, and/or public health and safety of the United States. These 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater.

Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. Among other things, this policy directive states that the federal government shall work with critical infrastructure owners and operators and state, local, tribal, and territorial entities to take proactive steps to manage risk and strengthen the security and resilience of the nation’s critical infrastructure. These efforts are to seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

Among the key risks facing the nation’s critical infrastructures are cybersecurity risks. Specifically, cyber systems supporting federal agencies and our nation’s critical infrastructures are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including via the internet. This increases the number of avenues of attack and expands their attack surface. As systems become more integrated, cyber threats pose an increasing risk to national security, economic wellbeing, and public health and safety.

Further, advancements in technology, such as data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data (including personally identifiable information) and track them across large and numerous databases. For example, social media has been used as a mass communication tool where personally identifiable information can be gathered in vast amounts.

In addition, ubiquitous internet and cellular connectivity makes it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of personally identifiable information being exposed and compromised.

Accordingly, ensuring the cybersecurity of both the public and private sector is an increasingly important effort. We have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure and, in 2015, to include protecting the privacy of personally identifiable information.[9]

Cybersecurity Incidents Affect Federal and Non-Federal Systems

Cybersecurity incidents pose a serious challenge to economic, national, and personal privacy and security. The following examples highlight the impact of such incidents:

- In December 2020, CISA issued an emergency directive and alert explaining that an advanced persistent threat actor had been observed leveraging, among other techniques, a software supply chain compromise[10] of an enterprise network management software suite.[11] According to CISA, the actor inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product. The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector

[9] See, most recently, GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[10] GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-20-171 (Washington, D.C.: Dec. 20, 2020). In this report, we found that few of the 23 civilian Chief Financial Officers Act agencies had implemented selected foundational practices for managing information and communications technology supply chain risks. For example, none of the 23 agencies fully implemented all of the selected supply chain risk management practices, and 14 of the 23 had not implemented any of the practices. We also found that the agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains. Accordingly, we made 145 recommendations to the 23 agencies to fully implement the foundational practices in their organization-wide approaches to information and communications technology supply chain risk management.

[11] DHS Emergency Directive 21-01 and CISA Alert AA20-352A.

organizations. CISA's alert further explained that the advanced persistent threat actor had demonstrated complex intrusion techniques, and the agency expects that removing this threat actor from compromised environments will be highly complex and challenging. According to CISA, this threat poses a grave risk to federal, state, local, tribal, and territorial governments as well as critical infrastructure entities and other private-sector organizations. Subsequently, in December 2020, the Federal Bureau of Investigation, CISA, and the Office of the Director of National Intelligence formed a Cyber Unified Coordination Group to coordinate a government response to the significant and ongoing cybersecurity campaign.

- In its 2020 annual data breach investigations report, Verizon reported analyzing 32,002 security incidents, identified across 81 countries in the 12 months since its 2019 report.[12] Of these incidents, 3,950 were confirmed to be data breaches.[13] Further, according to the report, more than a quarter of breaches go undiscovered for months or more.
- In February 2020, the Department of Justice announced that four members of the Chinese People's Liberation Army were indicted for allegedly hacking into the computer systems of the credit-reporting agency Equifax. In July 2017, Equifax system administrators discovered that cyber attackers had gained unauthorized access via the internet to the online dispute portal that maintained documents used to resolve consumer disputes. The Equifax breach resulted in the attackers accessing the personal information of at least 145.5 million individuals, including individuals' names, Social Security numbers, birth dates, addresses, and driver's license numbers.
- Between May and July 2019, the Defense Information Systems Agency network was breached, potentially compromising personal information, including Social Security numbers.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation stated that, since at least March 2016, hackers acting on behalf of the Russian government had targeted U.S. government agencies and critical infrastructure sectors, including the energy,

[12] Verizon, *2020 Data Breach Investigation Report-13th Edition* (May 2020).

[13] A data breach can be defined as an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security.

nuclear, water, aviation, and critical manufacturing sectors.

These concerns are further highlighted by the number of information security incidents reported by federal executive branch civilian agencies to CISA.[14] For fiscal year 2019, 28,581 such incidents were reported by the Office of Management and Budget (OMB) in its 2019 annual report to Congress, as mandated by the Federal Information Security Modernization Act of 2014 (FISMA).[15] These incidents included, among others, web-based attacks, phishing,[16] and the loss or theft of computing equipment. Further, the Federal Bureau of Investigation's Internet Crime Complaint Center reported receiving 467,361 complaints in 2019 from non-public entities, with the reported losses from these information security incidents exceeding $3.5 billion. The most prevalent crime types were phishing, non-payment/non-delivery, extortion, and personal data breach.

DHS Previously Established the National Protection and Programs Directorate to Carry Out Its Cybersecurity and Infrastructure Protection Responsibilities

The Homeland Security Act of 2002 created DHS and gave the department wide-ranging responsibilities for, among other things, leading and coordinating the overall national critical infrastructure protection effort.[17] In March 2007, DHS established NPPD to protect the nation's critical infrastructure from physical and cyber threats.

NPPD consisted of five divisions which executed its major functions:

[14] CISA includes a central federal information security incident center that compiles and analyzes information about incidents that threaten information security, known as CISA Central.

[15] The Federal Information Security Modernization Act of 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).

[16] Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

[17] See, generally, Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135-2321 (Nov. 25, 2002).

- The Office of Cybersecurity and Communications had the mission of ensuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
- The Office of Infrastructure Protection led the coordinated national effort to reduce risk to critical infrastructure posed by acts of terrorism.
- The Office of Cyber and Infrastructure Analysis provided consolidated all-hazards consequence analysis focusing on cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the nation's critical infrastructure.[18]
- The Federal Protective Service (FPS) protects and delivers law enforcement to and protection services for federal facilities.[19]
- The Office of Biometric Identity Management (OBIM), formerly US-VISIT, provides biometric identity services to DHS and its mission partners.[20]

Many of NPPD's activities were guided by the National Infrastructure Protection Plan (NIPP).[21] NPPD developed the plan through a collaborative process involving critical infrastructure stakeholders. It issued the plan in accordance with requirements set forth in the Homeland Security Act, as amended, as well as Homeland Security

[18] The Office of Cyber and Infrastructure Analysis was replaced by the National Risk Management Center in 2018.

[19] In response to the CISA Act of 2018, FPS was relocated to the DHS Management Directorate.

[20] In response to the CISA Act of 2018, OBIM was relocated to the DHS Management Directorate.

[21] The plan, originally developed in 2006, defines the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort. DHS issued the most recent version of the NIPP in 2013. The NIPP is a statutory requirement under 6 U.S.C. section 652(e)(1)(E), and CISA continues to use the plan to guide its approach to infrastructure protection.

Presidential Directive (HSPD)-7 and its successor PPD-21—*Critical Infrastructure Security and Resilience*.[22]

Central to the NIPP is managing the risks from significant threats and hazards to physical and cyber critical infrastructure, requiring an integrated approach to

- identify, deter, detect, disrupt, and prepare for threats and hazards to the nation's critical infrastructures;
- reduce vulnerabilities of critical assets, systems, and networks; and
- mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Among other things, the plan stresses a sector partnership model to coordinate critical infrastructure protection efforts at the federal, state, regional, local, tribal, territorial, and international levels, as well as between public- and private-sector partners. As part of this partnership model, each sector has an SCC, which is to represent a broad base of owners, operators, associations, and other entities within a sector, and a GCC, formed as the government counterpart to the SCC to enable interagency and cross-jurisdictional coordination.

The GCC consists of representatives across various levels of government (federal, state, local, tribal, and territorial), as appropriate to the security landscape of each sector. Each GCC is chaired by a representative from the corresponding sector-specific agency (SSA)—a federal agency with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector. The partnership model also includes cross-sector

[22] Homeland Security Presidential Directive (HSPD) 7 further defined critical infrastructure protection responsibilities for DHS and other departments. For example, HSPD-7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across critical infrastructure sectors. Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003). Presidential Policy Directive-21 succeeded HSPD-7 and established national policy on critical infrastructure security and resilience. It also refined and clarified the critical infrastructure-related functions, roles, and responsibilities across the federal government, as well as enhancing overall coordination and collaboration. Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013).

councils, regional coordinating councils, and a Critical Infrastructure Partnership Advisory Council, among other elements.

In addition to its responsibilities for ensuring the security of critical infrastructures, NPPD also carried out certain DHS responsibilities with respect to the cybersecurity of federal agencies and networks. In particular, DHS is responsible for certain operational aspects of agencies' information security policies and practices. These include issuing binding operational directives; monitoring agencies' security policies and practices, and assisting them with implementation; and assisting OMB in fulfilling its FISMA responsibilities.

GAO Previously Made Recommendations to Improve the Operations of CISA's Predecessor Agency

We previously reported on aspects of NPPD's operations and challenges it faced in carrying out its mission. For example:

- In July 2010, we reported on private- and public-sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent those expectations were being met.[23] We noted that private-sector stakeholders had reported that they expected their federal partners to provide usable, timely, and actionable cyber threat information and alerts; access to sensitive or classified information; a secure mechanism for sharing information; security clearances; and a single centralized government cybersecurity organization to coordinate government efforts. However, according to private-sector stakeholders, federal partners were not consistently meeting these expectations. For example, less than one-third of private-sector respondents reported that they were receiving actionable cyber threat information and alerts to a great or moderate extent. Public-sector stakeholders reported that they expected the private sector to provide a commitment to execute plans and recommendations, timely and actionable cyber threat information and alerts, and appropriate staff and resources. However, public-sector stakeholders stated that improvements could have been made to the partnership, including improving private-sector sharing of sensitive information.

  We made two recommendations, aimed at the national Cybersecurity Coordinator and DHS, to work with their federal and private-sector

[23] GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed,* GAO-10-628 (Washington, D.C.: July 15, 2010).

partners to enhance information-sharing efforts. DHS implemented the two recommendations.

- In October 2015, we testified regarding factors to consider for the then-potential reorganization of NPPD.[24] These factors included key questions to consider when evaluating an organizational change that involves consolidation; the need to balance executive and legislative roles; high-risk areas that agency officials should consider; and achieving greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation. In this testimony, we noted that, given the critical nature of NPPD's mission, considering key factors from our previous work could help inform an effective reorganization effort. For example, the lessons learned by other organizations involved in substantial transformations could provide key insights for agency officials as they considered and implemented the reorganization. We noted that attention to these and the other factors we identified could improve the chances of a successful NPPD reorganization.
- In February 2017, we reported that NPPD's National Cybersecurity and Communications Integration Center (NCCIC)[25] had taken steps to perform each of its 11 statutorily required cybersecurity functions, such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities.[26] However, the extent to which NCCIC adhered to nine statutorily defined implementation principles when performing the functions was unclear because the center had not determined the applicability of the principles to all 11 functions, or established metrics and methods by which to evaluate its performance against the principles. In addition, we identified factors that impeded NCCIC's ability to more efficiently perform several of its cybersecurity functions, such as an inability to completely track and consolidate cyber incidents reported to the

[24] GAO, *National Protection and Programs Directorate: Factors to Consider when Reorganizing,* GAO-16-140T (Washington, D.C.: Oct. 7, 2015).

[25] In 2009, DHS developed an integration center, the NCCIC, to provide a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats. The National Cybersecurity Protection Act of 2014 required NCCIC to perform several cybersecurity functions, including being a federal civilian interface for sharing information on cybersecurity-related information and facilitating cross-sector coordination to address cybersecurity risks and incidents. Prior to the CISA Act, NCCIC was part of NPPD's Office of Cybersecurity and Communications.

[26] GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

center, thereby inhibiting its ability to coordinate the sharing of information across the government.

Accordingly, we recommended that DHS take nine actions to enhance the effectiveness and efficiency of NCCIC, including to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments. As of February 2021, DHS had implemented three of the nine recommendations.

CISA Developed an Organizational Transformation Initiative to Implement Changes Needed to Carry Out Its Mission

The CISA Act of 2018 established the agency with responsibilities for leading national cybersecurity and critical infrastructure protection efforts, as well as requiring certain organizational changes. To implement these requirements and position itself to effectively carry out its mission, CISA launched an organizational transformation initiative to be carried out in three phases.

The Cybersecurity and Infrastructure Security Agency Act of 2018 Renamed NPPD and Specified Organizational Changes and Mission Responsibilities

Following approximately a decade of operation, NPPD staff, DHS officials, and members of Congress identified a need to streamline and consolidate NPPD to further its mission of protecting the nation's critical infrastructure. Accordingly, in November 2018, Congress passed, and the president signed, the CISA Act of 2018.[27]

The act renamed NPPD the Cybersecurity and Infrastructure Security Agency (CISA), prescribed changes to its organizational structure, and assigned the agency specific responsibilities to focus on cybersecurity and critical infrastructure protection efforts. These responsibilities include, among others,

[27] CISA Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169, section 2202(a)(1) (codified at 6 U.S.C. section 652).

- leading cybersecurity and critical infrastructure security programs, operations, and associated policy, including national cybersecurity asset response activities;
- coordinating with federal entities, including sector-specific agencies, and non-federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the agency, as appropriate;
- carrying out the responsibilities of the Secretary of Homeland Security to secure federal information and information systems consistent with law;
- coordinating a national effort to secure and protect against critical infrastructure risks; and
- providing analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, providing those analyses, expertise, and other technical assistance in coordination with sector-specific agencies and other federal departments and agencies.

The key requirements of the CISA Act of 2018 are summarized in table 1.

Table 1: Key Requirements of the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018

Required organizational elements

- CISA must be led by a Director and Deputy Director.
- CISA must have a Cybersecurity Division, Infrastructure Security Division, and Emergency Communications Division.
- CISA must have a Privacy Officer.
- The Office of Biometric Identity Management must be relocated to the Department of Homeland Security Management Directorate, and the department must determine an appropriate placement for the Federal Protective Service.

Key responsibilities assigned to CISA

- Secure federal information and information systems
- Coordinate national efforts to secure and protect against critical infrastructure risks

- Coordinate with federal and nonfederal entities, including international partners
- Respond to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance as needed
- Carry out emergency communications responsibilities under existing law

Source: GAO analysis of the CISA Act of 2018. | GAO-21-236

In particular, the act laid out a general structure for CISA, outlined its key responsibilities, described roles and responsibilities for its senior leadership, and directed that three divisions be established. The act also provided authority for relocating certain NPPD offices (FPS and OBIM) that were not to be part of CISA's core cybersecurity, emergency communications, and infrastructure security mission.

CISA Developed a Three-Phase Organizational Transformation Initiative to Determine and Implement Necessary Changes

To implement the requirements of the CISA Act of 2018, CISA leadership launched an organizational transformation initiative, which included three phases. The goals of this initiative included unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.

CISA's organizational transformation initiative was to comprise three phases, which were to define and implement the changes needed to meet the requirements of the act and position CISA to effectively carry out its mission.

- Phase one was intended to determine the organizational changes to meet its mission needs and respond to the requirements of the act. It was to include an internal review of NPPD's mission, culture, procedures, structure, and opportunities for improvement. Activities included exploratory design discussions carried out with groups of NPPD employees organized around twelve "lines of effort" (e.g. functions and programs, human capital, regional operations, and morale and culture). The output of this phase was to include a set of recommendations to address issues related to these lines of efforts, as well as an initial proposed organizational structure for the agency.
- Phase two was intended to validate the proposed changes made as a result of phase one and make any needed modifications in

consultation with internal and external CISA stakeholders. Activities included gathering feedback from employees and CISA component offices regarding their proposed organizational structures and concepts of operations. They also included benchmarking with similar reorganizations previously carried out within DHS, as well as informing congressional committees regarding proposed changes and the progress of the initiative.

- Phase three was intended to identify, validate, and execute tasks needed to fully implement the planned organizational changes. While CISA 2020 was to serve as the central coordinator for phase three, each organizational element was to be responsible for executing tasks and ensuring follow-through. This effort was to include the development of a high-level implementation task list to guide the overall effort and validation of these tasks with agency division and mission-support subject matter experts; cross-agency collaboration to execute the identified tasks; and tracking progress and sharing information through various communication channels.

Taken together, the three phases were intended to make the necessary changes to CISA's organization to enable it to effectively carry out its mission. CISA originally intended to complete the transformation by December 31, 2020.

CISA Has Made Progress in Implementing Its Organizational Transformation Initiative but Has Experienced Delays

CISA completed the first two phases of its organizational transformation initiative, including defining an organizational structure in accordance with its statutory responsibilities. In addition, the agency has defined its program and service delivery approach, which includes more centralized functions, consolidated stakeholder engagement, and expanded regional activities, among other things. Nevertheless, while the agency has taken actions toward implementing its planned organizational changes, it has encountered delays on some phase three activities. CISA officials attributed these delays to a variety of factors, although they told us the COVID-19 pandemic has generally had minimal impact on their efforts.

CISA Has Fully Completed Phase One and Two of Its Transformation Initiative, Which Included a New Organizational Structure and Service Delivery Approach

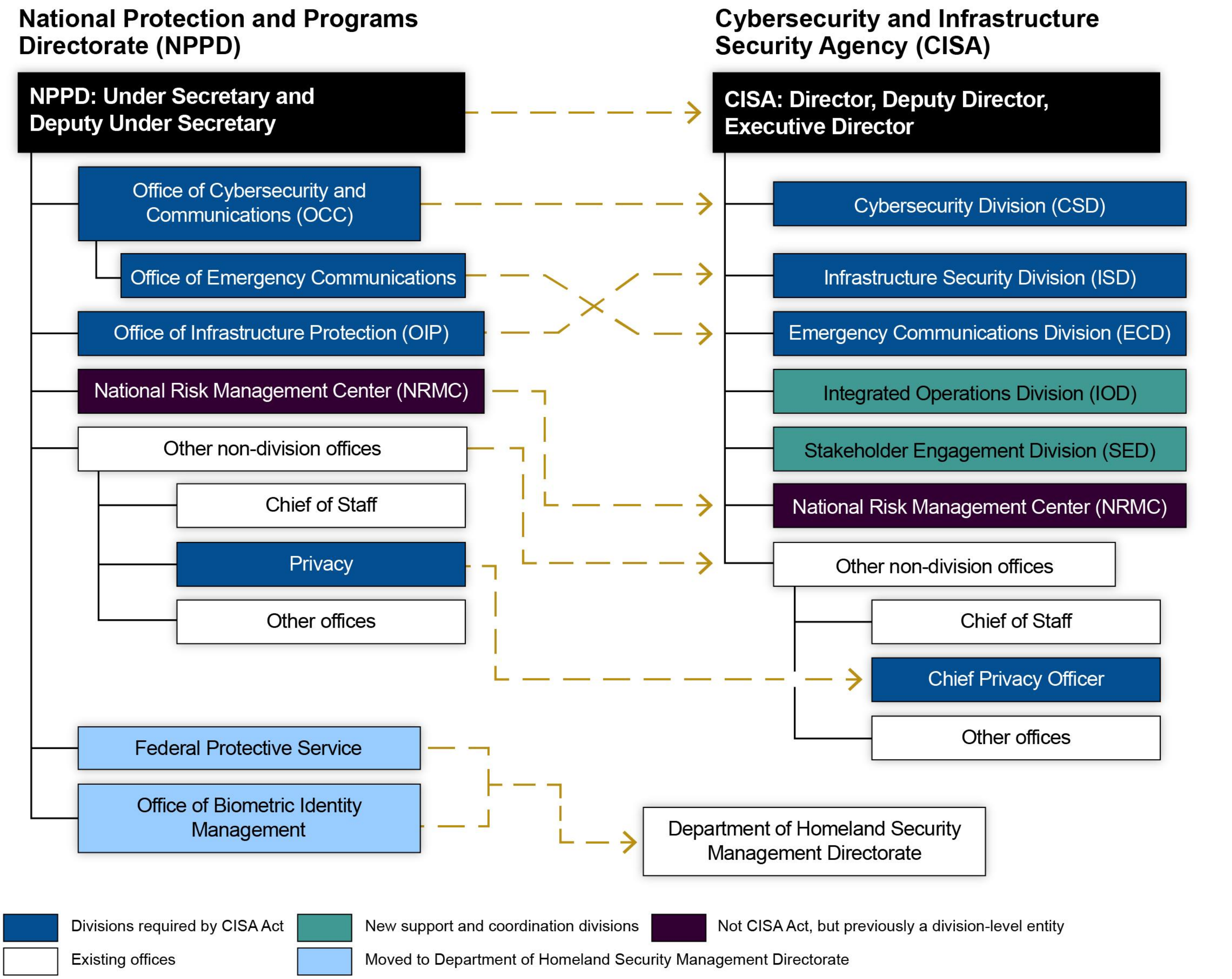
CISA took a number of actions, as part of the first two phases of its organizational transformation initiative, to define its new organization structure and establish the agency's mission.

- Phase one (conducted between July 2018 and January 2019) was organized around twelve lines of effort (e.g., functions and programs, human capital, regional operations, and morale and culture) with corresponding groups of NPPD employees leading the exploratory design discussions. The discussions took place during a 90-day study in anticipation of the passage of the CISA Act of 2018. The output of this effort was more than 80 recommendations, summarized in a document titled *CISA 2020: Forging a New Future—Conceptual Blueprint for Organizational Change Management*. The recommendations addressed goals such as successfully equipping the organization, supporting the mission, aligning resources with leadership priorities, unifying the agency through clear and consistent messaging, organizing the enterprise to enhance mission effectiveness, and attracting and retaining the critical workforce. The report also included the agency's mission and vision statements, next steps for proceeding with the organizational changes, and an initial proposed organizational structure.
- During phase two (conducted between February 2019 and June 2019), CISA took steps to validate and modify the proposals generated during phase one. This included holding 43 "listening sessions" that engaged more than 520 employees. These sessions led to a series of findings and recommendations aimed at guiding the organizational transformation. In addition, the CISA 2020 team solicited input from the agency's component offices, such as its major divisions, regarding their organizational structures and concepts of operation. Further, CISA benchmarked its plans against other DHS component agencies and briefed congressional committees on its efforts during this phase.

CISA Established an Organizational Structure That Aligned with Its Key Responsibilities Outlined by the Act

As a result of these first two phases of its organizational transformation efforts, CISA has developed an organizational structure that includes three statutorily defined divisions that are to carry out its mission, as well as key leadership and support offices. The organizational structure also includes three divisions not explicitly named in the act, which are intended to provide cross-agency support and integration. Figure 1 shows the key changes from the past NPPD organizational structure to the new CISA organizational structure.

Figure 1: Changes from NPPD Organization Structure to CISA Organization Structure


National Protection and Programs Directorate (NPPD)
Cybersecurity and Infrastructure Security Agency (CISA)
NPPD: Under Secretary and Deputy Under Secretary
CISA: Director, Deputy Director, Executive Director
Office of Cybersecurity and Communications (OCC)
Cybersecurity Division (CSD)
Office of Emergency Communications
Infrastructure Security Division (ISD)
Office of Infrastructure Protection (OIP)
Emergency Communications Division (ECD)
National Risk Management Center (NRMC)
Integrated Operations Division (IOD)
Other non-division offices
Stakeholder Engagement Division (SED)
Chief of Staff
National Risk Management Center (NRMC)
Privacy
Other non-division offices
Other offices
Chief of Staff
Chief Privacy Officer
Other offices
Federal Protective Service
Office of Biometric Identity Management
Department of Homeland Security Management Directorate
Divisions required by CISA Act
New support and coordination divisions
Not CISA Act, but previously a division-level entity
Existing offices
Moved to Department of Homeland Security Management Directorate

Source: GAO analysis of CISA data. | GAO-21-236

Under the new organizational structure, CISA is led by a Director and Deputy Director. In addition, the agency established the position of Executive Director as a senior career executive to oversee execution of the Director and Deputy Director's vision for CISA operations and mission support, and provide continuity during presidential transitions. Further, the organization includes three divisions mandated by the CISA Act of

2018—the Cybersecurity Division, the Infrastructure Security Division, and the Emergency Communications Division. These three statutory divisions are led by Executive Assistant Directors and have oversight and decision-making authority over such matters as policy, program management, program standards, capability development, doctrine, performance measures, and other functions associated with their statutory responsibilities.

CISA leadership also established three divisions not named in the act—the Stakeholder Engagement Division, Integrated Operations Division, and National Risk Management Center. Each of these divisions, which is led by an Assistant Director, is tasked with enabling effective coordination of activities that cut across the entire organization. These activities include coordinating operations among divisions and within regions, providing a unified field reporting structure, and managing stakeholder relationships, among other activities.

In addition, CISA has established a number of mission support offices that report directly to the Director and Deputy Director. These include the Offices of the Chief Counsel, Chief Information Officer, Chief Information Security Officer, Chief Financial Officer, Chief Human Capital Officer, Chief Learning Officer, Privacy Officer, Chief Security Officer, Chief Technology Officer, and Chief of Contracting Office, among others. According to the CISA Deputy Director, consolidating and elevating these functions was intended to provide more consistent and accountable mission support for the agency.

Table 2 provides more details on CISA's divisions, including related statutory responsibilities and key functions.

Table 2: Cybersecurity and Infrastructure Security Agency (CISA) Statutory and Support and Coordination Divisions

	Division	Related statutory responsibilities	Key activities
Statutory Divisions	Cybersecurity Division	Securing federal information and information systems	• Protecting federal civilian government networks • Collaborating with the private sector to increase the security of critical networks • Detecting and analyzing threat activity, preventing threats through information sharing and technical means, and responding to cybersecurity incidents
	Infrastructure Security Division	Directing the critical infrastructure security efforts of the agency	• Helping critical infrastructure owners/operators and other partners address risks to critical infrastructure • Providing tools and training to help manage the risks to their assets, systems, and networks
	Emergency Communications Division	Carrying out emergency communications responsibilities	• Leading the nation's public safety, national security, and emergency preparedness communications efforts • Providing training, coordination, tools, and guidance to help partners develop their emergency communications capabilities
Support and Coordination Divisions	Integrated Operations Division	Ensuring that all the agency's externally facing activities are coordinating, collaborating, and communicating across divisions to allow for seamless support and fast response to critical needs	• Providing a single reporting channel to give leadership end-to-end operational visibility for physical, cyber, and emergency communications activities • Serving as the primary service delivery function for customers, operating under the direction of the 10 regional directors
	Stakeholder Engagement Division	Enabling the coordination of stakeholders, fostering collaboration and a culture of shared ownership, managing priorities and performance, and coordinating with international partners	• Managing the customer relationship management platform • Collecting strategic stakeholder feedback and requirements • Implementing the National Infrastructure Protection Plan public-private partnership framework
	National Risk Management Center	Working with key stakeholders to identify, understand, and address the nation's highest priority critical infrastructure risks, originating from cyberattacks and other hazards	• Identifying and analyzing current and emerging risks • Collaborating with stakeholders on the highest priority risks, to include such topics as election security, supply chain security, fifth-generation (5G) wireless networks, and pipeline cybersecurity

Source: GAO analysis of agency data. | GAO-21-236

CISA's Service Delivery Approach Includes Consolidation of Functions, Centralized Coordination, and Increased Regional Activities

As part of its organizational transformation efforts and the establishment of its new organizational structure, CISA has taken steps to define its product and service delivery model. These steps include consolidating certain functions, centralizing its coordination with stakeholders, and increasing its regional activities.

CISA has consolidated certain functions in order to provide a more unified and consistent approach throughout the agency. For example:

- **CISA Central:** The agency created CISA Central to be the unified portal and point of contact for critical infrastructure partners and stakeholders to contact CISA and request assistance.[28] According to officials, CISA Central serves as the central point within the agency where internal staff and external stakeholders can exchange any type of security information with the agency. Rather than forcing stakeholders to go to multiple points within CISA for cyber, communications, or physical information needs, CISA Central is intended to be a one-stop-shop to request information sharing support or to distribute information to federal, state, local, tribal, and territorial stakeholders across the range of CISA's mission space.
- **Watch floor consolidation:** CISA has combined its three watch floors, which are integrated operations centers for information sharing and incident response coordination among the federal government and its various partners. The three watch floors (the NCCIC,[29] the

[28] https://www.cisa.gov/central.

[29] In 2009, DHS developed an integration center, the National Cybersecurity and Communications Integration Center (NCCIC), to provide a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats. The National Cybersecurity Protection Act of 2014 required NCCIC to perform several cybersecurity functions, including being a federal civilian interface for sharing information on cybersecurity-related information and facilitating cross-sector coordination to address cybersecurity risks and incidents. Prior to the CISA Act of 2018, NCCIC was part of NPPD's Office of Cybersecurity and Communications.

National Infrastructure Coordinating Center (NICC),[30] and the National Coordinating Center for Communications (NCC)[31]) correspond to the cybersecurity, physical infrastructure, and emergency communications domains, respectively. These are consolidated within CISA's Integrated Operations Division in order to establish comprehensive operational visibility and enable an integrated approach to cyber and physical threat monitoring, and can be contacted through CISA Central.

- **Consolidation of cyber and physical exercises:** CISA conducts cyber and physical exercises with federal, state, local, tribal, territorial, private-sector, and international partners to enhance the security and resilience of critical infrastructure. These exercises are intended to provide stakeholders with effective and practical mechanisms to examine plans and procedures, potentially identify areas for improvement, and share best practices. The exercises may also inform future planning, technical assistance, training, and education efforts. As part of the organizational transformation, CISA has combined its cyber and physical exercise teams to ensure a more unified and consistent approach.
- **Service and product catalog:** CISA has also developed a new catalog of its products and services to inform the agency's stakeholders of available services, encourage information sharing within the community, and promote the protection of physical and digital systems.[32] CISA's products and services include a variety of risk management and response services to build stakeholder resiliency and form partnerships. Specific examples of services and products that CISA provides include webinars and other training, tabletop exercises, technical tools, risk and vulnerability assessments, and technical assessments, among others. These services and

[30] The NICC is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information-sharing hub to support the security and resilience of these vital assets.

[31] The NCC continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes and earthquakes. In cases of emergency, NCC Watch leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework.

[32] CISA, *Cybersecurity and Infrastructure Security Agency Services Catalog*, accessed on December 7, 2020, https://www.cisa.gov/publication/cisa-services-catalog.

products are organized into four categories corresponding to key CISA mission areas: cybersecurity, infrastructure security, emergency communications, and risk management. They are then further broken down by focus area, or the type of activity the service performs. Table 3 describes these product types.

Table 3: Cybersecurity and Infrastructure Security Agency (CISA) Product Types

Product type	Description
Capacity Building	Efforts aimed at developing capabilities or human skills within a community or organization to reduce the level of risk or the effects of an incident negatively impacting physical and/or cyber infrastructure
Emergency Communications	Communications used by all federal, state, local, tribal, territorial and industry partners, emergency responders and government officials for coordination of emergency response planning and support
Incident Management and Response	The process by which all levels of government, nongovernmental organizations, and the private sector work together to prevent, protect against, mitigate, respond to, and recover from incidents
Information and Data Sharing	The exchange of data between various organizations, people and technologies to improve resilience of stakeholder owned and operated critical infrastructure
Partnership Development	Increasing collaboration between all levels of public and private-sector partners to improve resilience, awareness, and support of stakeholders
Risk Assessment and Analysis	The process of identifying risks to organizational operations, assets, and individuals; and the process to comprehend the nature and severity of the risk and act accordingly

Source: CISA. | GAO-21-236

CISA has also centralized its stakeholder management functions in the Stakeholder Engagement Division. As previously mentioned, this division is intended to provide a centralized, unified approach to managing CISA's stakeholder relationships. Specifically, the division is intended to

- foster collaboration and shared stakeholder ownership through the implementation and communication of aligned engagement priorities, governance, processes, standards of practice, feedback loops, performance management, and analytics;
- transform mission delivery and stakeholder experience by facilitating a consistent and coordinated enterprise stakeholder engagement approach using a customer relationship management platform with interoperability with other agency systems;
- maximize the value of subject-matter experts and build/ strengthen partnerships through a unified sector-specific agency management approach; and

- broaden CISA's reach and position as a thought leader through the development of strategic and collaborative partnerships.

Another element of CISA's service delivery model is an increased use of its regional staff. CISA is increasing its regional presence in the form of staff who work directly with critical infrastructure partners and communities at the regional, state, tribal, and local level. These staff include local and regional Protective Security Advisors, Cybersecurity Advisors, Emergency Communications Coordinators, and other CISA personnel. These personnel are to advise and assist in training and exercises, as well as in disseminating best practices to support partners in achieving more robust resilience.

The regional staff are managed out of the Integrated Operations Division (with the exception of Emergency Communications Coordinators, who are managed out of the Emergency Communications Division). This division is intended to function as a single reporting channel to give leadership end-to-end operational visibility for physical, cyber, and emergency communications activities and serve as the primary service delivery function for customers. According to the CISA Deputy Director, this approach allows the agency to work directly with infrastructure owners and operators, such as smaller businesses, which may not be heavily involved in in coordinating councils and trade groups.

CISA Is Currently in Phase Three of Its Transformation Initiative, but Significant Delays Have Occurred; Officials Did Not Identify Significant Impacts from COVID-19

Phase three of CISA's organizational transformation is intended to fully implement the planned organizational changes. To carry this out, CISA developed an implementation task list consisting of 13 initiatives. The implementation task list identified a list of work tasks for each of the 13 initiatives and assigned a "CISA 2020 Steward" responsible for each initiative. Originally, the agency's goal was to fully implement these tasks by the end of calendar year 2020.

As of mid-February 2021, CISA had completed 37 of the 94 tasks on the most recent version of its task list, with 57 tasks remaining to be completed. Of the tasks not completed, 42 were past their most recent planned completion dates. In addition, several of the planned completion dates have been delayed until the first quarter of 2021, and a few moved until later in 2021. Further, many of the planned completion dates had been revised between January and November 2020, with the new dates exceeding the original dates from 60 to 822 days. Table 4 summarizes the status of the implementation tasks. (Appendix II provides further details on the status of the implementation tasks.)

Table 4: Status of Cybersecurity and Infrastructure Security Agency (CISA) Phase Three Implementation Tasks as of Mid-February 2021

Implementation initiative	Total number of tasks	Tasks completed	Tasks remaining	Percent complete
Acquisition and procurement	3	0	3	0
Administrative services	6	0	6	0
Budget and finance	4	1	3	25
Communication and branding	4	4	0	100
Federal Protective Service-Office of Biometric Identity Management Transition	2	2	0	100
Functions and programs	22	11	11	50
Human capital	19	0	19	0
Information technology	7	2	5	29
Legislative requirements	7	7	0	100
Morale and culture	4	2	2	50
Regional operations	2	0	2	0
Stakeholder engagement	3	1	2	33
Vision and strategy	11	7	4	64
Totals	**94**	**37**	**57**	**39**

Source: GAO analysis of CISA data. | GAO-21-236

Among the work tasks that CISA had completed as of mid-February 2021 were:

- defining and finalizing the new organizational structure and completing the table of organization to determine the placement of all CISA personnel;
- aligning the agency’s budget with its new organizational structure; completing the transition of FPS and OBIM to the DHS management directorate;
- establishing branding guidance;
- developing the CISA vision and mission statement and issuing the agency’s strategic intent; and

- meeting legislative requirements for updating Congress on aspects of the organizational transformation.

Tasks that remained to be completed included:

- finalizing the set of mission-essential functions for each division;
- issuing a memorandum defining incident management roles and responsibilities across CISA;
- preparing and issuing the CISA Concept of Operations;
- completing the realignment of program and mission support personnel;
- launching a revitalized workforce planning capability;
- determining requirements for centralized business systems across the agency;
- establishing CIO functions and structures that support integrated services with sufficient flexibility to meet requirements across headquarters and regional elements;
- establishing the Chief Information Security Officer functions and structures;
- maturing the planning, programming, budgeting, and execution process;
- implementing a workforce engagement plan; and
- fully defining and implementing the agency's stakeholder engagement approach.

A number of these incomplete tasks appear to be critical to CISA's transformation initiative and accordingly the ability to effectively and efficiently carry out its cyber and critical infrastructure protection mission. For example, finalizing the set of mission-essential functions for each division and completing the realignment of program and mission support personnel will help ensure that critical mission functions are fully defined and that the agency has the workforce in place to carry them out. In addition, issuing a memorandum defining incident management roles and responsibilities across CISA would provide an improved understanding of staff's expected incident management roles and allow CISA to more efficiently detect and respond to incidents.

Regarding the delays, in November 2020, two CISA officials, the Deputy Director and the former Chief of Transformation, stated that some of the more significant tasks, particularly those related to finalizing the organizational structure and the mapping of program personnel, had taken longer than anticipated because of the need to obtain buy-in from various stakeholders. For example, they stated that input from Congress required additional clarification of the organizational structure. The officials also noted that some other delays were due to coordination with DHS leadership and the Office of Management and Budget taking longer than CISA anticipated, which was necessary to get buy-in on the agency's revised organizational structure.

Further, because some tasks took longer than anticipated, the officials stated this may have had cascading effects on later tasks that were dependent on earlier ones. The officials added that they believed it was important to ensure that certain tasks were done right, particularly those that would impact CISA employees, even if this might have resulted in delays. Finally, these officials stated that they expected all the major activities to be completed by the end of December 2020, although they acknowledged some tasks would not be completed until sometime in 2021.

However, as of mid-February 2021, CISA had not fully updated its task list with current planned completion dates for all activities, and had not undertaken any re-prioritization of the remaining tasks due to the delays that have occurred. In addition, CISA officials did not identify an updated overall target completion date for the organizational transformation. Leading practices and standards for comprehensive planning emphasize the need for agencies to identify the time frames for defined objectives and to assess their progress toward achieving their objectives. Given the organizational transformation was developed in part to improve the agency's mission effectiveness, ensuring that the effort is completed in a timely fashion is critical to meeting this goal.

Significant recent cyber incidents and ongoing threats further highlight the importance of CISA's role in leading the national effort to understand and manage cyber and physical risk to our critical infrastructure and, consequently, the need to complete its organizational transformation. Reassessing its implementation plan and the associated schedule would assist CISA in identifying realistic time frames for the remaining tasks to be completed, better positioning the agency to achieve the goals of its transformation initiative and effectively carry out its critical mission.

CISA Officials Identified Minimal Impact of COVID-19 on Their Efforts

CISA officials told us in July 2020 that the COVID-19 pandemic had had minimal impact on the progress of their organizational transformation efforts. The CISA Deputy Director attributed this to the fact that the transformation initiative was already into phase three when the agency went to full remote work in March 2020. He added that, if the agency had been in phase one or two, it would have been much more difficult because of the need for collaboration and listening sessions. The Assistant Director of the Stakeholder Engagement Division added that the pandemic response had accelerated the timeline by which the agency had to convene its partners. He also stated that the response required CISA to bring stakeholders together to look at problems, such as regional effects, and to focus on information sharing through a very specific lens. Further, he added that this had tested the agency's processes for unity of effort and unity of message, and for requesting information—requiring a demonstration of processes that, otherwise, would have been done piecemeal.

In November 2020, CISA officials, including the Deputy Director, noted that the COVID-19 pandemic had made some things more challenging, particularly in ironing out the fine details of the reorganization. The officials added that the pandemic had probably led to additional delays. They reiterated that the pandemic had required them to test their stakeholder outreach model, and that the results of their efforts had provided a validation of the organizational structure.

CISA Generally Addressed Four Key Practices for Organizational Transformation, Partially Addressed Five, and Did Not Address One

Through our prior work, we have identified key practices for effective agency reforms (which include organizational transformations).[33] This

[33] GAO-18-427. As mentioned previously, with respect to these practices, "reforms" broadly includes any organizational changes—such as major transformations, mergers, consolidations, and other reorganizations—and efforts to streamline and improve the efficiency and effectiveness of government operations.

work has shown that successful reforms or transformations depend upon following change management practices, such as agreement on reform goals, and the involvement of the Congress, federal employees, and other key stakeholders. The practices we used to assess CISA's organizational transformation efforts are shown in table 5.[34] (See app. III for the full list of key practices and associated key questions we used in our assessment.)

Table 5: Selected Categories and Subcategories of GAO's Key Practices for Assessing Agency Reforms

Category	Subcategory	Description
Goals and outcomes	Establishing goals and outcomes	Agency reforms should clearly identify what an agency is trying to achieve by establishing clear outcome-oriented goals and performance measures that enable the agency to assess the extent to which projects are achieving progress toward its goals. This process should also include considering how the changes align with the agency's mission and strategic plan, considering costs and benefits, and identifying any short- and long-term efficiency initiatives.
Process for developing the reforms	Involving employees and key stakeholders	It is important for agencies to directly and continuously involve not only their employees but also key stakeholders in the development of major reforms. These stakeholders may include congressional stakeholders, customers, other agencies, and other external partners. Agencies should incorporate the feedback received from stakeholders into the agency's proposed changes.
	Using data and evidence	In undertaking a major reform or reorganization, agencies are better equipped when basing their efforts on data and evidence, such as from program evaluations or performance data. This includes identifying the data or evidence the agency is using to justify its proposed changes and determining that the evidence is sufficiently reliable to support the case for the changes. Agencies can also incorporate results from their strategic review and enterprise risk management processes.
	Addressing fragmentation, overlap, and duplication	In our prior work, we have identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing or better managing programmatic fragmentation, overlap, and duplication. In undertaking reforms or reorganizations, agencies should identify potential areas of fragmentation, overlap, and duplication, as well as whether its proposals or reform efforts could address these areas and yield any cost savings.
	Addressing high-risk areas and long-standing management challenges	Reforms improving the effectiveness and responsiveness of the federal government often require addressing long-standing weaknesses in how some federal programs and agencies operate. As part of the reform efforts, agencies should identify high-risk issues or other challenges their efforts are intended to address, as well as how they intend to monitor the effects of their efforts on these challenges.

[34] These agency reform practices are organized into four categories and 12 subcategories. For our purposes, we identified 10 subcategories as the key practices we used to assess CISA's organizational transformation efforts. We determined that the subcategories of Determining the Appropriate Role of the Federal Government and Workforce Reduction Strategies were not applicable to our assessment because the role of the federal government with regard to CISA was established by law and because CISA is not undertaking workforce reductions as part of its reform effort.

Category	Subcategory	Description
Implementing reforms	Ensuring leadership focus and attention	Organizational transformation should be led by a dedicated team of high-performing leaders within the agency. This includes identifying leaders and an implementation team, making a compelling case for change, and ensuring accountability in implementing the changes.
	Managing and monitoring	Agencies should carefully and closely manage organizational transformations by developing an implementation plan with key milestones and deliverables to track and communicate implementation progress, among other actions. This also includes putting processes in place to collect data for measuring the reform's outcome-oriented goals and plans to measure customer satisfaction with the changes resulting from its reforms.
Strategically managing the federal workforce	Strengthening employee engagement	Increased levels of employee engagement–generally defined as the sense of purpose and commitment employees feel toward their employer and its mission–can lead to better organizational performance and can sustain or increase levels of employee engagement and morale, even as employees weather reorganization and other difficult external circumstances. To do so, agencies should develop plans to strengthen and sustain employee engagement during and after the reforms and managing diversity and ensuring an inclusive work environment.
	Conducting strategic workforce planning	Agencies should conduct strategic workforce planning, which is an essential activity for ensuring that an agency's human capital program aligns with its current and emerging mission and programmatic goals, and that the agency is able to meet its future needs. This includes assessing the effects of the proposed organizational changes on the agency's workforce and conducting strategic workforce planning to determine whether it will have the needed resources and capacity, including the skills and competencies, in place.
	Ensuring effective employee performance management	Performance management systems–which are used to plan work and set individual employee performance expectations, monitor performance, develop capacities to perform, and rate and incentivize individual performance–can help the organization manage employees on a daily basis and provide supervisors and employees with the tools they need to improve performance. In carrying out reforms or reorganizations, agencies should align their employee performance management system with the goals of the planned changes and ensure that it creates incentives for high-performing employees and addresses employees with unacceptable performance.

Source: GAO. | GAO-21-236

As summarized in table 6, CISA's organizational transformation efforts generally addressed four of the selected key reform practices, partially addressed five, and did not address one.

Table 6: Extent to Which the Cybersecurity and Infrastructure Security Agency's (CISA) Organizational Transformation Efforts Addressed Selected Agency Reform Practices

Key practice	Extent addressed
Establishing goals and outcomes	Partially addressed
Involving employees and key stakeholders	Partially addressed
Using data and evidence	Generally addressed
Addressing fragmentation, overlap, and duplication	Partially addressed
Addressing high-risk areas and long-standing management challenges	Generally addressed

Key practice	Extent addressed
Ensuring leadership focus and attention	Generally addressed
Managing and monitoring	Partially addressed
Strengthening employee engagement	Generally addressed
Conducting strategic workforce planning	Partially addressed
Ensuring effective employee performance management	Not addressed

Legend: Generally addressed – CISA addressed this practice without significant gaps in its coverage of the actions associated with the subcategory.

Partially addressed – CISA addressed this practice with significant gaps in its coverage of the actions associated with the subcategory.

Not addressed – CISA did not address this practice or demonstrate coverage of actions associated with the subcategory.

Source: GAO analysis of agency data. | GAO-21-236

CISA generally addressed four of the selected practices:

- **Using data and evidence:** CISA established 12 discrete employee discussion groups that served as the primary means to explore issues, gather inputs, and solicit feedback from its leaders and employees on organizational capabilities and requirements for the future state of the organization. The output of the discussion groups was used to inform the case made to DHS leadership and congressional stakeholders for the proposed organizational changes.
- **Addressing high-risk areas and long-standing management challenges:** As part of its organizational transformation, CISA identified and addressed several previously identified high-risk areas and long-standing management challenges. A key planning document titled *CISA 2020: Forging a New Future-Conceptual Blueprint for Organizational Change Management*, identified long-standing management challenges and weaknesses that the reorganization is intended to address. The document also laid out the major organizational change concepts intended to address these challenges and weaknesses.
- **Ensuring leadership focus and attention:** The agency tasked the Deputy Director with overseeing the organizational transformation; appointed a Chief of Transformation to manage the implementation; established mechanisms to hold leadership accountable for the initiative; and established a dedicated implementation team to manage the process with support from contractors.
- **Strengthening employee engagement:** CISA established an Office of Workforce Engagement, developed various mechanisms for feedback and communication with the workforce, undertook various initiatives intended to manage diversity and ensure an inclusive work environment, and utilized the Federal Employee Viewpoint Survey data to determine employees' satisfaction throughout the

reorganization.

CISA partially addressed the selected practices in five areas:

- **Establishing goals and outcomes:** CISA defined three broad outcome-oriented goals for the organizational transformation: unify the agency, improve mission effectiveness, and enhance the workforce. In addition, the agency has shown how its plans to align with its mission and strategic plan and has included both short-term and longer-term efficiency initiatives in its proposed reforms. For example, CISA has established the Integrated Operations Division and Stakeholder Engagement Division to create efficiencies in field reporting, unifying operations, and interacting with stakeholders.

  However, while CISA identified three outcome-oriented goals for the reorganization, it has not yet developed performance measures to gauge the extent to which its efforts meet these goals. CISA officials told us that the agency's Performance and Evaluation Office has been tasked with developing such measures in 2021, but they did not provide a specific timetable. Until the agency establishes detailed plans for the development of outcome-oriented performance measures, CISA's ability to assess the effectiveness of its efforts and their impact on its mission activities, such as leading efforts to identify and manage cyber risks, will be limited.

- **Involving employees and key stakeholders:** CISA involved employees in its organizational transformation efforts through a variety of mechanisms. For example, CISA solicited input from its workforce through focus groups, surveys, listening sessions, and requests for information, which allowed employees to provide input into the design of the reorganization. The agency has also held numerous town halls throughout its reform effort, which have allowed CISA to discuss with its employees its mission, vision, guiding principles, and the progress between the phases. In addition, CISA has kept congressional committees updated on its reform efforts and provided multiple briefings that discussed its transformation process, organizational structures, consolidation of headquarters facilities, and work with sector-specific agencies.

  However, CISA did not provide evidence of the extent to which it has considered state, local, tribal and territorial officials and other sector stakeholders' views in the design of the reorganization. For example, CISA provided documentation showing that the agency presented aspects of the reorganization during various coordinating council and other stakeholder meetings, but it did not provide documentation that stakeholder input was collected or used to inform aspects of the organizational transformation.

In November 2020, CISA officials, including the Deputy Director and Stakeholder Engagement officials, told us that while they sought to inform various stakeholder groups about the shape of the reorganization, they did not believe it was necessary to use input from these stakeholders to drive decisions about the reorganization. This was, in part, because major aspects of the reorganization were driven by the requirements of the CISA Act of 2018.

However, as later discussed in more detail, stakeholders that we spoke with told us that they were not informed about aspects of the reorganization, leading to challenges in coordinating with CISA. Ensuring that organizational changes take into account the input of all internal and external stakeholders could help CISA increase customer acceptance of any changes and enhance the effectiveness of its coordination with critical stakeholders.

- **Addressing fragmentation, overlap, and duplication**: CISA officials identified a number of areas of fragmentation, overlap, and duplication in the pre-CISA organization, including multiple teams conducting physical and cyber exercises instead of a unified exercise team; fragmented chains of command for field operations; multiple watch floors; and decentralized mission support functions.[35] As part of its organizational transformation efforts, CISA developed initiatives that are intended to reduce potential fragmentation, overlap, and duplication, such as combining its physical and cyber exercise teams, consolidating its watch floors, and establishing centralized mission-support functions. According to agency officials, they expect that these efforts will result in reduced fragmentation, overlap, and duplication as part of their efforts to unify agency operations.

  However, the agency has not yet defined processes for monitoring the effects of these efforts or identifying potential cost savings resulting from them. CISA officials said they intended to do so in the future but

[35] Each year, GAO identifies and reports on federal agency programs with fragmented, overlapping, or duplicative goals or activities and ways to reduce costs or enhance revenue. See most recently, GAO, *2020 Annual report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Billions in Financial Benefits,* GAO-20-440SP (Washington, D.C.: May 19, 2020), and https://www.gao.gov/duplication/overview.

had not identified specific plans or time frames for these actions. Until it develops such processes, CISA may be unable to determine the effectiveness of its initiatives to reduce fragmentation, overlap, and duplication and identify resulting cost savings or other benefits.

- **Managing and monitoring:** CISA had developed and maintained an implementation task list for managing and monitoring its organizational transformation process. The list includes tasks under 13 transformation projects with associated milestones and deliverables and is used to track implementation progress.

  However, the agency had not defined processes to measure the outcomes of the organizational transformation or to assess customer satisfaction with the changes. CISA officials stated that they intend to identify "measurement factors" to be used in satisfaction surveys, but did not identify specific plans, including time frames, for doing so. Until the agency establishes such processes, it may be hindered in its ability to determine the effectiveness of its reorganization in meeting the needs of its customers and stakeholders, and thus its ability to effectively carry out its mission.

- **Conducting strategic workforce planning:** As required by law, CISA conducted an assessment of its cybersecurity workforce in 2019, which included an overview of the CISA Cybersecurity workforce, cybersecurity capabilities and work roles of critical need, its Cyber Talent Management System, and its Cybersecurity Workforce Strategy. According to the resulting report, CISA is working to analyze the current gaps in the cybersecurity workforce and develop a framework to determine the criticality of work roles to better assess and address capability gaps.

  However, CISA noted in its report that additional work was required to move toward becoming a more operational agency, working to meet the operational needs and requirements of the risk environment. This included gathering additional data and taking additional steps to identify and address gaps in its cyber workforce. Further, the agency had not undertaken strategic workforce planning for the agency as a whole. CISA officials stated that, once the reorganization is fully implemented, they expect to be in a better position to conduct such an assessment. The officials added that the agency had taken steps, including contracting for a manpower assessment, to be completed in the spring of 2021. However, the agency did not provide documentation of these efforts. Given the significance of recent cyber incidents and other risks facing the nation's critical infrastructure, it is essential that CISA plan for a workforce that aligns with its current and emerging mission and programmatic goals.[36]

Finally, CISA did not address the selected practice in the area of **ensuring effective employee performance management.** Specifically, CISA had not aligned its performance management system at all staff levels with the goals of the organizational transformation, or created incentives and rewards for top performers, while ensuring that it deals with poor performers.

According to CISA officials, leading change has been incorporated as a formal element in evaluating the performance of senior executive service staff, with explicit CISA 2020 guidelines added to the evaluations of every staff who reports directly to the Deputy Director. The officials added that expectations are transmitted from executive staff to staff employees throughout the agency. However, the agency did not provide documentation of these steps. Without such an alignment, CISA may be hindered in its ability to manage its employees and provide supervisors and employees with the tools needed to improve performance and effectively carry out its mission.

Selected Stakeholders Reported Challenges in Coordinating with CISA, and the Agency Has

[36] In April 2020, we reported on the implementation of several government-wide reform initiatives, including an initiative to address the cybersecurity workforce shortage. We reported that the Office of Management and Budget (OMB) and DHS partially addressed most leading practices through their efforts to implement several projects, such as reskilling employees to fill vacant cybersecurity positions, and streamlining hiring processes. However, we found that OMB and DHS have not established a dedicated implementation team, or a government-wide implementation plan, among other practices. We recommended that the Director of OMB, working with DHS, should develop a government-wide workforce plan that assesses the effects of the reform proposal to solve the cybersecurity workforce shortage on the current and future federal workforce. OMB did not respond to this recommendation. See GAO, *Federal Management: Selected Reforms Could Be Strengthened by Following Additional Planning, Communication, and Leadership Practices,* GAO-20-322 (Washington, D.C.: Apr. 23, 2020).

Developed Strategies to Address Some of These Challenges

Federal law and policy emphasize the importance of coordination and collaboration among federal agencies, other levels of government, and the private sector to manage risks to the nation's critical infrastructure and other assets.[37] This includes sharing timely, actionable information about risks and helping private-sector partners gain a more thorough understanding of the entire risk landscape, thus, enhancing their ability to make informed and efficient security and resilience investments. Accordingly, effective coordination with stakeholders is critical to carrying out CISA's mission. This coordination has become even more significant during the national response to the COVID-19 pandemic.

Selected stakeholders in CISA's three primary mission areas—protecting federal networks, critical infrastructure protection, and emergency communications—provided a variety of perspectives on their coordination with CISA. While all of them identified potential areas for improvement, the critical infrastructure stakeholders—government coordinating councils (GCC) and sector coordinating councils (SCC)[38]—more consistently reported challenges.

Specifically, the six federal CIOs we spoke with did not generally identify challenges in coordinating with CISA, though two noted that timeliness of responses to requests for information could be improved and two said the agency's new organizational structure could be better clarified. Similarly, the selected emergency communications stakeholders did not generally

[37] See: Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013) and Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013). According to these documents, DHS must incorporate expertise and day-to-day engagement from the Sector Specific Agencies (SSAs) as well as the specialized or support capabilities from other federal departments and agencies, and strong collaboration with critical infrastructure owners and operators and state, local, tribal, and territorial entities. In addition, the CISA Act of 2018 specifically requires CISA to coordinate with a variety of stakeholders, including SSAs; other federal agencies; state, local, tribal, and territorial government entities; and the private sector, in carrying out its mission.

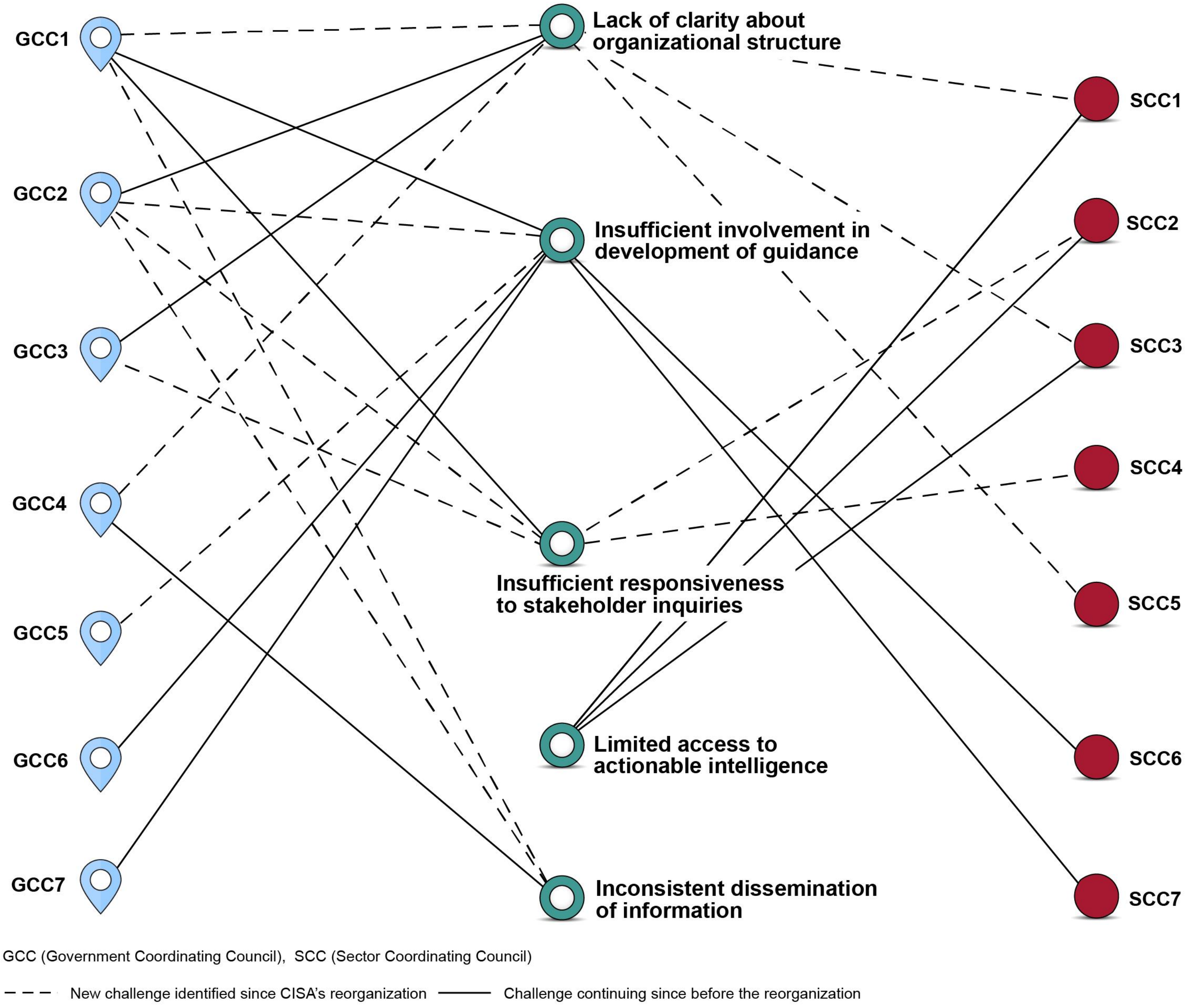
[38] These stakeholders included 16 critical infrastructure stakeholders (eight representatives of selected Sector Coordinating Councils and eight representatives from selected Government Coordinating Councils), six federal Chief Information Officers (CIO), and six State-wide Interoperability Coordinators and other emergency communications stakeholders.

identify challenges, although three noted that they perceived that cybersecurity was receiving increased attention from CISA compared with emergency communications and interoperability.

In contrast, stakeholders from 14 of the 16 critical infrastructure sectors (seven SCCs and seven GCCs) reported a number of coordination challenges. These challenges were in five broad areas: (1) lack of clarity on changes to CISA's organizational structure, (2) lack of involvement in developing stakeholder guidance, (3) lack of timely responses to stakeholder requests, (4) inconsistent distribution of information, and (5) lack of access to actionable intelligence.

Figure 2 depicts which of these challenge areas the selected SCC and GCC representatives identified as affecting their coordination with CISA, including whether this was a new challenge since CISA's reorganization or had been a challenge prior to the reorganization and continued after. Further discussion of each challenge area follows the figure.

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors


GCC1
GCC2
GCC3
GCC4
GCC5
GCC6
GCC7
Lack of clarity about organizational structure
Insufficient involvement in development of guidance
Insufficient responsiveness to stakeholder inquiries
Limited access to actionable intelligence
Inconsistent dissemination of information
SCC1
SCC2
SCC3
SCC4
SCC5
SCC6
SCC7
GCC (Government Coordinating Council), SCC (Sector Coordinating Council)
New challenge identified since CISA's reorganization
Challenge continuing since before the reorganization

Source: GAO analysis of stakeholder responses. | GAO-21-236

- **Lack of clarity on changes to CISA's organizational structure:** Critical infrastructure stakeholders reported that they were not informed of the new CISA organizational structure and how it would affect who they should be coordinating with. Specifically, seven of 16 critical infrastructure stakeholders mentioned this challenge, with five stating this was a new challenge since the reorganization and two stating that it has been an issue since before the reorganization and continued to the present. For example, one stakeholder's primary challenge in this area was understanding which offices within CISA are responsible for which areas or programs, resulting in inefficiencies and delays in their communication with CISA. Another stakeholder said that since they had never been provided a new organization chart for CISA, they were unsure who to contact at the agency related to a program that conducts inspections on facilities in their sector. The stakeholder added that this has led to additional and unnecessary back-and-forth communication when a member of the council has an issue with this inspection program.

With regard to this challenge, CISA officials stated that, while the organizational structure of the agency has changed, the program leads and contact points generally have not. They added that they have taken steps to make it easier for stakeholders to access CISA services and assistance. For example, CISA Central, the agency portal for customer interactions, is intended to be a consistent "front door" for interactions with the agency, and the service catalog, which lists available CISA services and products, is intended to make it easier for partners and potential partners to see what services CISA provides. The officials noted that they believe this increased the agency's transparency to stakeholders.

However, the uncertainty expressed by these seven stakeholders suggests that CISA has not sufficiently communicated changes associated with the reorganization so that stakeholders know with whom they should be coordinating for specific issues and programs. Further, the critical infrastructure stakeholders we spoke with told us that they were not asked to provide formal input into the reorganization, which may have created confusion regarding the new organizational structure and corresponding points of contact.

The NIPP emphasizes the importance of clear and frequent communication as part of a well-functioning partnership for critical infrastructure protection. Without additional communication on the new organizational changes, stakeholders will continue to be hindered in their ability to effectively coordinate with CISA. This lack of clarity could have consequences for CISA's ability to work effectively with these stakeholders to respond to a cyber incident or other critical need.

- **Lack of involvement in developing stakeholder guidance:** Stakeholders reported that they were not included early enough in the process of developing guidance that impacted their sectors. Specifically, seven of 16 critical infrastructure stakeholders stated that they experienced this challenge, with two stating this was a new challenge since the reorganization and five stating that it has been ongoing since before the reorganization. For example, one stakeholder stated that CISA had produced guidance describing the protection of educational facilities that included information on which their sector had specific expertise, without providing them the opportunity to ensure the information in the guidance was accurate. The stakeholder stated that not involving sector subject matter experts in the development of guidance can lead to incomplete or incorrect information being released to members of the sector. Another stakeholder said that they were given opportunities to provide input to guidance documents, but their input was not always included in the final version of the product, and it was unclear why some input was accepted and some was not.

  CISA officials stated that they regularly engage with stakeholders when developing guidance. For example, when working on a specific topic, they may stand up a working group and have discussions that lead to the development of joint products. The officials added that this is consistent with the partnership model articulated in the NIPP. However, the officials also stated that there seems to be an increasing expectation from stakeholders that their input will be "operationalized" and that they will have greater levels of input from the very beginning of guidance development. CISA officials acknowledged that stakeholders have been asking for greater involvement and stated they are currently working on a new version of the NIPP, which is expected to revisit the partnership model, including stakeholder engagement.

  However, while CISA officials indicated that the NIPP revision would address stakeholder relationships, they did not provide details on whether it would address the issue of inconsistent involvement of stakeholders in developing guidance for their sectors. Currently, the NIPP specifies that the federal sector-specific agency (SSA) or co-SSA assigned to each sector is to have institutional knowledge and specialized expertise about its sector and should coordinate with DHS in its critical infrastructure protection mission. However, stakeholders from different sectors indicated varying levels of involvement in the guidance development process, and that without this involvement, guidance developed by CISA did not always reflect the specialized expertise that SSAs can offer. Without more consistent engagement with all stakeholders, CISA could be missing opportunities to incorporate sector-specific expertise and develop guidance tailored to the needs of the various sectors.

- **Lack of timely responses to stakeholder requests:** Stakeholders reported problems in receiving timely responses from CISA to inquiries about data they submitted for data calls and other issues the sectors deemed critical. Specifically, five of 16 critical infrastructure stakeholders stated that they experienced this challenge, with four stating this was a new challenge since the reorganization and one stating that it has been ongoing since before the reorganization. For example, a stakeholder stated that it took three-and-a-half weeks to get a high-level summary of results based on a survey asking what problems their sector had been experiencing. Without timely information, the stakeholder stated that it is more difficult for them to do their jobs. Another stakeholder stated that they needed to wait for a high-level CISA official to approve emergency guidance, and the delay in disseminating this guidance put their stakeholders at risk of not receiving timely information to combat a particular threat.

  CISA Stakeholder Engagement officials noted that they have multiple efforts under way to ensure effective follow up on stakeholder inquiries. First, the officials said they are working to develop a unified workflow mechanism to track inquiries received via CISA Central in order to ensure the inquiries receive timely responses. Second, to address stakeholder concerns, the officials said they have begun developing more timely briefings for stakeholders based on information collected, although they added that some of the data collected are used primarily for internal government decision making rather than for stakeholder products. Timeliness in responding to stakeholders may continue to be an ongoing issue until CISA completes its current efforts; but if implemented effectively they should help address this challenge.

- **Inconsistent distribution of information:** Stakeholders reported that they did not always receive information from CISA that was intended to be shared with their respective sectors. Among the stakeholders we spoke to, this challenge was only identified by GCCs, who are responsible for, among other things, coordinating strategic communications, discussion, and resolution of issues among government entities within their sectors. Specifically, three of the eight GCC stakeholders stated that they experienced this challenge, with two stating this was a new challenge since the reorganization and one stating that it has been ongoing since before the reorganization. For example, two of these stakeholders stated that email distribution lists used by CISA to disseminate important information were incomplete or outdated. As a result, they were not always aware of information to be shared with their respective sectors, or missed requests for information from CISA or other important notifications. For example, one stakeholder noted that CISA held a workshop detailing the threats to their sector; however, key federal stakeholders did not receive notification about the workshop and, therefore, were not able to send comprehensive representation. As a consequence, this stakeholder said they were not able to fully respond to the concerns of private-sector stakeholders that were raised at the workshop.

CISA officials told us they do not perceive inconsistent information distribution as a challenge because their teams coordinate monthly with all the sector specific agencies, which act as the GCC chairs. Further, the officials stated that CISA is required, as a compliance requirement under the Critical Infrastructure Partnership Advisory Council, to maintain accurate records about who chairs the various councils and other entities, and that distribution lists are updated on a regular basis and published quarterly.

However, as of November 2020, CISA had not provided documentation of these coordination efforts. Additionally, critical infrastructure stakeholders told us that CISA had not formally solicited their input on this challenge. Such inaction could perpetuate a gap between CISA's and stakeholders' understanding of the accuracy and effectiveness of the methods relied on for communication. The NIPP emphasizes the importance of clear and frequent communication as part of a well-functioning partnership for critical infrastructure protection. Without ensuring that information is consistently communicated, CISA may be hindered in ensuring that all key stakeholders are receiving needed information to manage risks to critical infrastructure. This could hinder stakeholders' ability to respond to adverse events, such as cyber incidents or vulnerabilities, in a timely and effective manner.

- **Lack of access to actionable intelligence:** Private-sector stakeholders reported limited access to classified information or declassified versions of actionable intelligence collected by the government that may affect their sectors. This challenge was identified only by SCCs we spoke with, which as private-sector entities are less likely to have the clearances required to access classified information. Specifically, three of these eight SCC stakeholders stated that they had experienced this challenge, with all three stating that it had been ongoing since before the reorganization. For example, these stakeholders stated that there were limited opportunities to receive unclassified versions of classified products that may help them address threats. They noted that, without access to complete information, stakeholders may not be able respond to emerging threats to critical infrastructure.

CISA officials cited this as a perennial challenge and said they were aware that there has always been a demand for access to timely, actionable intelligence. They noted that CISA uses classified information forums, specialized briefings, and classified briefings at the beginning of joint coordinating council meetings and works with every sector to develop “key intelligence questions” to help focus on what is significant to the sector and to ensure that products meet their needs. CISA provided examples of efforts to distribute classified information or information that has been declassified through these briefings on topics such as Hurricane Sally and cybersecurity threats. Access to classified information for private-sector stakeholders is an ongoing issue and the current efforts by CISA indicate that it is taking appropriate steps to address this challenge.

Selected Stakeholders Generally Had Positive Views of CISA’s Response to COVID-19

When evaluating CISA’s response to COVID-19, the selected stakeholders were generally positive when speaking about the agency’s overall handling of the crisis. Some stakeholders pointed out that the agency needed to better work out roles and responsibilities in such a crisis, especially with regard to Emergency Support Functions. Four of eight GCC representatives also noted that, while CISA had released relevant and useful guidance for the private sector, the agency could coordinate more closely with sector specific agencies to better include agency subject matter experts during the pandemic.

However, the stakeholders added that CISA was able to provide useful products and information, and in some cases was able to help procure particularly needed supplies such as personal protective equipment for the critical infrastructure sectors. Representatives from 15 of 16 GCCs and SCCs pointed to frequent calls organized by CISA to brief all the sectors on the current situation in the pandemic and the Essential Critical Infrastructure Workforce guidance as particularly useful products and services.

Conclusions

With the passage of the CISA Act, the agency has been engaged in a transformation initiative intended to establish an organizational structure in accordance with the act's requirements and position it to carry out its cybersecurity, infrastructure protection, and emergency communications missions. In accordance with its statutory responsibilities, CISA has established a new organizational structure, developed a service and product delivery approach, and taken steps to implement its planned organizational changes. However, delays have occurred in fully implementing the changes. Recent cyber incidents have highlighted the importance of fully implementing CISA's organizational changes so that it is positioned to lead national efforts to identify and manage cyber and other risks to critical infrastructure. By establishing completion dates for delayed phase-three tasks and an overall deadline for the completion of the transformation initiative, CISA will be better positioned to complete its organizational transformation without additional delays.

In addition, while CISA's plans for its organizational transformation generally addressed key practices for effective agency reforms in areas, gaps in addressing other key practices, such as establishing goals and outcomes and managing and monitoring its efforts, could hinder the full effectiveness of the agency's reorganization. Addressing each of key practices will better position CISA to ensure the success of its reorganization efforts and carry out its mission to lead national efforts to identify and respond to cyber and other risks.

Finally, critical infrastructure stakeholders we spoke to identified challenges that could hinder CISA's efforts to ensure effective coordination. CISA has taken actions to mitigate challenges in the areas of timely responses to stakeholder request and lack of access to actionable intelligence. However, it has not taken adequate actions in the areas of communicating organizational changes to stakeholders, involving stakeholders in the development of sector-specific guidance, and including appropriate parties in all communication channels. By assessing and enhancing aspects of its communication and collaboration with these stakeholders, CISA could help address challenges they identified and better ensure that they have the information needed to identify and respond to cyberattacks and other risks affective the nation’s critical infrastructure.

Recommendations for Executive Action

We are making the following 11 recommendations to CISA:

The Director of CISA should establish expected completion dates for those phase three tasks that are past their completion dates, with priority given to those tasks critical to mission effectiveness. (Recommendation 1)

The Director of CISA should establish an overall deadline for the completion of the transformation initiative. (Recommendation 2)

The Director of CISA should establish plans, including time frames, for developing outcome-oriented performance measures to gauge the extent to which the agency’s efforts are meeting the goals of the organizational transformation. (Recommendation 3)

The Director of CISA should collect input to ensure that organizational changes are aligned with the needs of stakeholders, taking into account coordination challenges identified in this report. (Recommendation 4)

The Director of CISA should establish processes for monitoring the effects of efforts to reduce fragmentation, overlap, and duplication including identifying potential cost savings. (Recommendation 5)

The Director of CISA should establish an approach, including time frames, for measuring outcomes of the organizational transformation, including customer satisfaction with organizational changes. (Recommendation 6)

The Director of CISA should develop a strategy for comprehensive workforce planning. (Recommendation 7)

The Director of CISA should take steps to align the agency’s employee performance management system with its organizational changes and associated goals. (Recommendation 8)

The Director of CISA should communicate relevant organizational changes to selected critical infrastructure stakeholders to ensure that these stakeholders know with whom they should be coordinating in CISA's organization. (Recommendation 9)

The Director of CISA should take steps, with stakeholder input, to determine how critical infrastructure stakeholders should be involved with the development of guidance for their sector. (Recommendation 10)

The Director of CISA should assess the agency's methods of communicating with its critical infrastructure stakeholders to ensure that appropriate parties are included in distribution lists or other communication channels. (Recommendation 11)

Agency Comments and Our Evaluation

DHS provided written comments on a draft of this report.[39] In its comments, which are reproduced in appendix IV, the department concurred with our recommendations and described steps planned or under way to address them.

For example, the department stated that CISA plans to create an updated task list with prioritized tasks and completion dates, and establish an overall deadline for the transformation initiative, by March 2021. DHS also specified actions that CISA plans to take to fully address the selected agency reform practices, including developing performance measures and developing and implementing a comprehensive workforce planning strategy. In addition, the department stated that CISA plans to address the challenges we identified in coordination with CISA's stakeholders by, for example, developing and implementing a mechanism to communicate organizational changes to selected critical infrastructure stakeholders and analyzing stakeholder distribution and communication channels.

With regard to our recommendation that CISA align its employee performance management system with its organizational changes and associated goals (recommendation 8), the department stated that CISA's Performance Management System aligns to the new organizational structure and has been approved by both the Office of Personnel Management and DHS. The department added that CISA had taken other steps, including a quarterly audit of employee performance work plans so

[39] As part of our outreach CISA stakeholders, we also gave selected federal agencies the opportunity to review excerpts from our draft report. These agencies did not have any comments on the draft excerpts.

that performance and contribution to the mission can be properly monitored and adjusted, as appropriate. For these reasons, the department requested that we consider this recommendation resolved and implemented.

However, documentation that CISA provided regarding its actions did not show how the agency's performance management system had been modified to align with the agency's organizational changes and goals. As a result, we intend to follow up with the agency to verify actions it has taken to address this recommendation. DHS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, the Acting Director of CISA, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Nathan J. Anderson at (206) 287-4804 or andersonn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Nick Marin

Nick Marinos
Director, Information Technology and Cybersecurity

Nathan Anderson

Nathan J. Anderson
Director, Homeland Security and Justice

List of Requesters

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ron Johnson
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kyrsten Sinema
Chair
Subcommittee on Government Operations and Border Management
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Tom Carper
United States Senate

The Honorable Mitt Romney
United States Senate

The Honorable Jacky Rosen
United States Senate

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to

6. describe the Cybersecurity and Infrastructure Security Agency's (CISA) organizational transformation initiative;
7. assess the progress of CISA's organizational transformation initiative, as well as any impact of the Coronavirus Disease 2019 (COVID-19) pandemic on these efforts;
8. determine the extent to which CISA's organizational transformation efforts align with key practices for effective agency reforms, including organizational transformations; and
9. identify challenges, if any, that exist in CISA's efforts to coordinate with government and private-sector stakeholders, and strategies the agency has developed to address these challenges.

To address our first objective, we analyzed requirements of the CISA Act of 2018 and other relevant laws, such as the Homeland Security Act of 2002, to identify the agency's key statutory responsibilities. We also reviewed CISA documentation, including reports, memoranda, and briefings, to understand the agency's organizational transformation initiative. Further, we interviewed agency officials, including the Deputy Director and the Chief of Transformation, to get their perspectives on the nature and goals of the organizational transformation initiative.

To address our second objective, we reviewed and analyzed relevant agency documents, including its Strategic Intent, documentation of the CISA 2020 Transformation Initiative, organization charts, and other documentation related to the three phases of the organizational transformation. We compared documentation of CISA's planned organizational changes to requirements in the CISA Act of 2018 related to the agency's organizational structure, as well as CISA documentation, including its preliminary organizational charts, budget overview and budget requests, information about CISA's divisions found on its website, CISA briefings to congressional committees on its planned organizational changes, and relevant prior GAO work. Based on this review, we determined what changes were made to the agency's organizational structure such as which National Protection and Programs Directorate functions and offices corresponded to new divisions within CISA and what functions they are intended to perform. We further identified aspects of CISA's approach to delivering products and services to its customers and stakeholders.

In order to track the progress of tasks associated with the implementation phase of CISA's transformation initiative, we reviewed and analyzed CISA's implementation task list and other pertinent agency documentation to determine if each task had been completed on or before its planned completion date. We also incorporated status updates and other comments provided by CISA. For each determination, a second analyst verified the supporting documentation. We also interviewed cognizant CISA officials, including the Deputy Director, Chief of Transformation, Assistant Director for Stakeholder Engagement, and Chief Human Capital Officer, to discuss organizational transformation efforts and the reasons for any delays, including the impact, if any of the COVID-19 pandemic on their efforts.

To address our third objective, we selected relevant key practices from those identified by GAO for assessing agency reforms.[1] With respect to these practices, "reforms" broadly includes any organizational changes—such as major transformations, mergers, consolidations, and other reorganizations—and efforts to streamline and improve the efficiency and effectiveness of government operations.

To select the relevant practices, we reviewed prior GAO work using these practices and, for each subcategory and key question, determined whether they were applicable to CISA's reorganization efforts based on factors including (1) the origins of the CISA reorganization in federal law; (2) the current status of CISA's reorganization efforts; (3) the nature of CISA's mission; (4) identified high-risk issues or issues of fragmentation, overlap, or duplication relevant to CISA; and (5) mandates, if any, for CISA to reduce its workforce. We excluded two subcategories because we determined that they were not applicable to CISA's efforts. Specifically, we excluded "determining the appropriate role of the federal government" because the establishment and reorganization of CISA was mandated by law and, thus, determining the appropriate role of the federal government is not within the scope of the agency's reorganization

[1] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts,* GAO-18-427 (Washington, D.C.: June 13, 2018).

efforts. We also excluded “workforce reduction strategies” because, according to CISA officials, the agency has not been required to reduce its workforce.

For each subcategory, we performed an initial assessment of documents and other evidence provided by CISA to determine the extent to which they addressed the subcategory. The assessment was based on whether CISA’s efforts addressed key implementation steps for each subcategory, based on an analysis of the key questions for that subcategory. After identifying any gaps, we requested additional information from and/or meetings with CISA officials as appropriate and incorporated the new information into our assessment.

Based on this assessment, we determined if CISA had generally, partially, or not addressed each subcategory. We determined that CISA generally addressed the practice if we did not identify significant gaps in its coverage of the actions associated with this practice, partially addressed the practice if we identified significant gaps in its coverage of the actions associated with this practice, and did not address the practice if it had not substantively addressed any of the actions associated with the practice. The initial assessment was reviewed by a second analyst to determine if they reached the same conclusions. In cases where the second analyst reached a different conclusion, the two analysts met to discuss and reconcile their assessments. All differences were reconciled without the need to go to a third party adjudicator.

To address our fourth objective, we interviewed 28 selected CISA stakeholder entities corresponding to CISA’s three statutorily defined mission areas: cybersecurity and the protection of federal civilian networks, critical infrastructure protection, and emergency communications.

For federal cybersecurity and network protection, we collected input from six members of the Federal Chief Information Officers (CIO) Council. These members were identified by the council as “core” CIOs who would be best positioned to answer questions on behalf of the council about coordination with CISA. These CIOs were from the Departments of Agriculture, Defense, Energy, Justice, and Labor, and the General Services Administration. We held a moderated group meeting with these officials and asked them questions about their relationship with CISA and challenges, if any, they had experienced in coordinating with CISA, both before and after the reorganization. (Representatives from the

Department of Defense were unable to attend the group discussion, but provided responses in writing.)

For critical infrastructure protection, we met with representatives of the 16 critical infrastructure sectors—eight government coordinating councils (GCC) and eight sector coordinating councils (SCC). This was done to ensure that we would get perspectives from both government and industry/private-sector stakeholders. Specifically, we met with the eight GCCs not chaired by the Department of Homeland Security (DHS), and with the SCCs from the eight remaining sectors. The GCCs and the respective agency chairs we met with were as follows: Defense Industrial Base (Department of Defense); Energy (Department of Energy); Financial Services (Department of Treasury); Food and Agriculture (Department of Agriculture & Department of Health and Human Services); Healthcare and Public Health (Department of Health and Human Services); Government Facilities (Federal Protective Service); Transportation Systems (Department of Transportation); and Water and Wastewater Systems (Environmental Protection Agency). The SCCs and the respective agency chairs we met with were as follows: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste Sector. For each sector, we conducted semi-structured interviews with stakeholders to understand their relationship with CISA and identify challenges, if any, they experienced in coordinating with CISA both before and after the reorganization.

For emergency communications, we identified stakeholders based on prior GAO work. We selected six entities: the Statewide Interoperability Coordinators (SWIC) from the three states with the largest number of disasters (California SWIC, Oklahoma SWIC, and Texas SWIC) and three public safety associations with emergency communications responsibilities (American Public Works Association, International Association of the Chiefs of Police, and the International Association of Fire Chiefs). For each stakeholder entity, we conducted semi-structured interviews to understand their relationship with CISA and identify challenges, if any, they experienced in coordinating with CISA both before and after the reorganization. We also asked all groups of stakeholders about their experiences working with CISA during the COVID-19 pandemic.

After meeting with these stakeholders, we compiled their responses and performed a content analysis to identify common challenges, the number of stakeholders who identified each type of challenge, and the impact of these challenges on the stakeholders' operations. We developed a network analysis to show the relationships among the various stakeholders and challenge categories we identified.

Once we analyzed the responses, we met with CISA officials responsible for the agency's transformation efforts and for stakeholder engagement to determine what strategies, if any, the agency had to mitigate these challenges. Further, we followed up via email with the stakeholders we interviewed to ask them to what extent CISA had solicited their feedback on challenges.

We conducted this performance audit from September 2019 to March 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Status of Cybersecurity and Infrastructure Security Agency (CISA) Phase Three Implementation Tasks

To fully implement its organizational transformation, CISA developed an implementation task list consisting of 13 initiatives with associated specific work tasks. Table 7 shows the status of tasks from the list with planned completion dates by mid-February 2021.

Table 7: Status of Cybersecurity and Infrastructure Security (CISA) Phase Three Implementation Tasks

	Task	Status
Acquisition and Procurement	Establish processes to include: deployment of acquisition experts to programs, increased transparency, and strengthened leadership engagement throughout the acquisition lifecycle	Not complete. No current planned completion date provided.
	Define procurement guidance and standard operating procedures that promote consistency throughout program lifecycle	Not complete. Now planned for completion by 9/30/22.
	Establish Office of the Chief of Contracting Officer to build capacity and capability to support future CISA Head of Contracting Authority	Not complete. Now planned for completion by 10/1/22
Administrative Services	Develop plan for physical movement of staff to align with program/mission support personnel realignment	Not complete. No current planned completion date provided.
	Execute plan for physical movement of staff to align with program/mission support personnel realignment	Not complete. Planned for completion by 5/31/21
	Issue plan for transition and consolidation of facilities to Department of Homeland Security (DHS) headquarters (HQ) at St. Elizabeth's	Not complete. No current planned completion date provided.
	Streamline and enhance access control at all CISA facilities	Not complete. No updated planned completion date provided; considered an "ongoing" task
	Establish centralized administrative functions with sufficient flexibility to meet requirements across HQ and regional elements	Not complete. No current planned completion date provided.
Budget and Finance	Mature planning, programming, budgeting, and execution process	Not complete. Now planned for completion by 9/9/21
	Issue memorandum describing process for linking strategic planning with budgeting	Not complete. No updated planned completion date provided

	Task	Status
	Complete realignment of program assessment and evaluation function from office of Strategy, Policy, and Plans to Chief Financial Officer	Complete
	Establish the operational requirements function for CISA	Not complete. No current planned completion date provided.
	Prepare to operate in new Program/Project and Activity (PPA) Structure	Complete
	Define desired program, project, and activity structure	Complete
	Coordinate with the Office of Management and Budget to update budget crosswalk from legacy to new agency structure and incorporate feedback, as required	Complete
	Coordinate with Congress regarding updated PPA structure and incorporate feedback, as required	Complete
	Complete alignment of budget and finance structures, processes, and doctrine to ensure consistent delivery that reflects federal best practices.	Not complete. No current planned completion date provided.
Communications and Branding	Finalize processes for coordinating messaging and ensuring unity across the agency	Complete
	Publish CISA communications guidance	Complete
	Develop tools and training to engage and align all employees with new CISA identity	Complete
	Complete enhancement of CISA digital presence	Complete
	Publish CISA branding guidance	Complete
	Federal Protective Service-Office of Biometric Identity Management Transition	
	Complete transition of Federal Protective Service	Complete
	Complete transition of Office of Biometric Identity Management	Complete
Functions and Programs	Request proposed organizational structures and de-conflict responses	Complete
	Issue memorandum on implementing the CISA operating model	Complete and removed from task list
	Finalize Senior Executive Service allocation, placement, and requirements	Complete
	Approve and disseminate CISA nomenclature memorandum	Complete
	Issue memorandum defining incident management roles and responsibilities across CISA	Not complete. In progress and no current planned completion date provided
	Publish approved CISA organizational structures	Complete
	Prepare and issue Concept of Operations by Division and Mission Support Offices	Not complete. No current planned completion date provided.
	Prepare and issue CISA Concept of Operations	Not complete. No current planned completion date provided.
	Establish tiger team and prepare plan for realignment of contracts across CISA	Canceled

	Task	Status
	Finalize set of mission essential functions associated with each division	Not complete. In progress and no current planned completion date provided
	Request mapping of legacy budget into new organizational structures	Complete
	Request mapping of program personnel to functions and organizational structures	Complete
	Reconcile overlaps, gaps, and issues, finalize mapping of all program personnel, and deliver to Chief Human Capital Officer for implementation	Complete
	Complete administrative realignment of program personnel and interim realignment of mission support personnel	Not complete. No updated planned completion date provided.
	Conduct cyberpay revalidation after program personnel realignment is complete	Not complete. No updated planned completion date provided.
	Conduct position description revalidation and remapping effort across CISA for program personnel	Not complete. No updated planned completion date provided.
	Identify current personnel performing mission support across CISA	Complete
	Determine mission support personnel requirements across CISA	Complete
	Reconcile overlaps, gaps, and issues, finalize mapping of all mission support personnel, and deliver to Chief Human Capital Officer for implementation	Complete
	Complete final administrative realignment of mission support personnel	Not complete. No current planned completion date provided.
	Conduct cyberpay revalidation after mission support personnel realignment is complete	Not complete. Now planned for completion by 3/31/21
	Conduct position description revalidation and remapping effort across CISA for mission support personnel	Not complete. Now planned for completion by 3/31/21
	Facilitate the internal communications of approved organizational changes to the CISA workforce as needed	Complete
	Make necessary personnel and accounting code systems adjustments	Not complete. In progress and no current planned completion date provided
Human Capital	Launch revitalized workforce planning capability, to include data analytics, forecasting, and requirements collection processes	Not complete. In progress and no current planned completion date provided
	Establish CISA Academy	Not complete. Now planned for completion by 10/1/21
	Establish career path and mentorship program	Not complete. In progress and no current planned completion date provided
	Establish leadership development program	Not complete. CISA reported this complete but has not provided supporting documentation

	Task	Status
	Establish Equal Employment Opportunity Officer	Not complete. No current planned completion date provided.
	Issue CISA Employee Training and Education System Concept of Operations	Not complete. Removed from task list
	Establish programs to enhance diversity and inclusion across the workforce	Not complete. In progress and no current planned completion date provided
	Finalize process for leveraging DHS HQ Civil Rights/Civil Liberties capabilities to support CISA	Not complete. No current planned completion date provided.
	Conduct preparation activities to launch CISA learning management system to track training across the organization to ensure readiness levels are maintained and skills strengthened	Not complete. Removed from task list.
	Establish Governance for a CISA Training and Education System	Not complete. In progress and no current planned completion date provided
	Establish Chief Learning Officer governance and oversight for agency-wide training and education partnerships	Not complete. No current planned completion date provided.
	Establishes Chief Learning Officer as central coordination and oversight for the National Workforce Training and Education Strategy & Program Evaluation for CISA	Not complete. No current planned completion date provided.
	Establish central coordination of training and evaluation outreach for CISA	Not complete. No current planned completion date provided.
	Stand Up the Office of the Chief Learning Officer Administratively	Not complete. In progress and no current planned completion date provided
	Establish human capital functions and structures that support integrated services with sufficient flexibility to meet requirements across headquarters and regional elements	Not complete. In progress and no current planned completion date provided
	Issue plan for revitalization and enhancement of recruitment and retention	Not complete. In progress and no current planned completion date provided
Information Technology	Determine requirements for centralized business systems across CISA	Not complete. No current planned completion date provided.
	Develop common definition and objectives for centralized business systems	Not complete. No current planned completion date provided.
	Identify required CISA centralized business systems	Not complete. No current planned completion date provided.
	Establish Chief Information Officer functions and structures that support integrated services with sufficient flexibility to meet requirements across HQ and regional elements	Not complete. No current planned completion date provided.

	Task	Status
	Establish CISA Chief Technology Officer functions and resources	Complete
	Issue CISA enterprise data management strategy	Complete
	Develop integrated enterprise architecture	Not complete. In progress and no current planned completion date provided
Legislative Requirements	Provide information on CISA stakeholder outreach mechanisms	Complete
	Provide briefing on mechanisms for collaboration among CISA and Sector Specific Agencies	Complete
	Provide report on efforts to consolidate CISA facilities, personnel, and programs	Complete
	Provide report on how CISA is meeting requirements under Cybersecurity Workforce Assessment Act	Complete
	Provide report on cloud-based security deployments for civilian federal departments/agencies	Complete
	Provide briefing on impacts of enhanced Sector Specific Agency collaboration	Complete
	Provide information on mechanisms for internal collaboration to further CISA operational coordination, integrated situational awareness, and improved integration across CISA	Complete
Morale and Culture	Transition all CISA internal communications and engagement functions to Workforce Engagement	Complete
	Implement Workforce Engagement Plan	Not complete. In progress and no current planned completion date provided.
	Establish cadre of engagement ambassadors	Complete
	Publish schedule of regular leadership communication and engagement to staff at all levels and in the regions and Headquarters	Complete
	Create employee feedback mechanisms	Complete and removed from task list
	Establish workforce recognition program	Complete
	Establish innovation lab	Not complete. Now scheduled for completion by 2/28/21.
	Establish the CISA Employee Store	Complete
Regional Operations	Issue memorandum defining CISA service delivery types and how services are delivered to stakeholders	Not complete. No current planned completion date provided.
	Publish guidance on regional reporting structures, required staffing, roles and responsibilities, and coordination processes between national and regional offices	Not complete. CISA reported this complete but has not provided supporting documentation.
Stakeholder Engagement	Issue memorandum defining Stakeholder Engagement roles and responsibilities across CISA	Not complete. No current planned completion date provided.
	Publish stakeholder engagement strategy to ensure consistent, unified, and prioritized engagement efforts	Not complete. Now scheduled for completion by 8/1/21

Task	Status
Implement Stakeholder Relationship Management (SRM) tool	Complete
Prepare and disseminate Integrated and Unified Stakeholder Relationship Information Management Memorandum	Complete
Establish a Stakeholder Relationship Management Task Force	Complete
Prepare standards, concept of operations, and CISA-wide implementation plan to achieve SRM tool final operating capability	Removed from task list.
Vision and Strategy	Complete
Issue final CISA Mission and Vision statements	Complete
Issue CISA Strategic Intent	Complete
Issue memorandum on Governance Framework	Complete
Publish interim set of policies and procedures to guide CISA administration and operations	Not complete. No current planned completion date provided.
Engage with CISA mission support offices to introduce the Governance Framework, gather feedback, and support them in the creation of policies and doctrine using the new standards	Complete
Engage with CISA divisions to introduce the Governance Framework, gather feedback, and support them in the creation of policies and doctrine using the new standards	Complete
Complete list of priority policy and doctrine for publishing in 2020	Complete
Issue Governance Framework, Policy System, and Doctrine System Directives and their associated instructions and Standard Operating Procedures	Complete
Issue Governance Framework Directive and Policy System Instruction	Complete
Issue Doctrine System Instruction	Complete
Rolling release of priority policies and doctrine	Not complete. Considered an ongoing task
Issue Enterprise Performance Risk Management System and Integrated Planning System Directives and related instructions.	Not complete. No current planned completion date provided.
Assess implementation of the Governance Framework and its components, and update standards as required	Not complete. No current planned completion date provided.

Source: GAO analysis of CISA data. | GAO-21-236

Appendix III: Key Questions for Assessing Agency Reform Efforts

We developed key questions based on our prior work on key practices that can help assess agency reform efforts or organizational transformations. The 58 questions are organized into four broad categories and 12 subcategories. We determined that 10 of the subcategories were applicable to the Cybersecurity and Infrastructure Security Agency's organizational transformation. The categories, subcategories, and associated key questions are shown in table 8.

Table 8: Key Questions for Assessing Agency Reform Efforts

Category	Subcategory	Key questions
Goals and outcomes	Establishing goals and outcomes	To what extent has the agency established clear outcome-oriented goals and performance measures for the proposed reforms?
		To what extent has the agency shown that the proposed reforms align with the agency's mission and strategic plan?
		To what extent has the agency considered and resolved any agency crosscutting or government-wide issues in developing their proposed reforms? For example, what are the implications of proposed reforms on other agencies?
		To what extent has the agency considered the likely costs and benefits of the proposed reforms? If so, what are they?
		To what extent has the agency considered how the upfront costs of the proposed reforms would be funded?
		To what extent has the agency included both short-term and long-term efficiency initiatives in the proposed reforms?
Process for developing the reforms	Involving employees and key stakeholders	How and to what extent has the agency consulted with the Congress, and other key stakeholders, to develop its proposed reforms?
		How and to what extent has the agency engaged employees and employee unions in developing the reforms (e.g., through surveys, focus groups) to gain their ownership for the proposed changes?
		How and to what extent has the agency involved other stakeholders, as well as its customers and other agencies serving similar customers or supporting similar goals, in the development of the proposed reforms to ensure the reflection of their views?
		How and to what extent has the agency considered the views of state and local governments that would be affected by the proposed reforms?
		How and to what extent have agencies gathered the views of the public and incorporate these views in the proposed reforms?

Category	Subcategory	Key questions
		Is there a two-way continuing communications strategy that listens and responds to concerns of employees regarding the effects of potential reforms?
		How will the agency publicize its reform goals and timeline and report on its related progress?
	Using data and evidence	What data and evidence has the agency used to develop and justify its proposed reforms?
		How has the agency determined that the evidence contained sufficiently reliable data to support a business-case or cost benefit-analysis of the reforms?
		How, if at all, were the results of agency’s strategic review process used to help guide the proposed reforms?
		How, if at all, were the results of agency’s enterprise risk management process used to help guide the proposed reforms?
	Addressing fragmentation, overlap, and duplication	To what extent has the agency addressed areas of fragmentation, overlap, and duplication—including the ones we identified—in developing its reform proposals?
		To what extent have the agency reform proposals helped to reduce or better manage the identified areas of fragmentation, overlap, or duplication?
		To what extent has the agency identified cost savings or efficiencies that could result from reducing or better managing areas of fragmentation, overlap, and duplication?
	Addressing high-risk areas and long-standing management challenges	What management challenges and weaknesses are the reform efforts designed to address?
		How specifically has the agency considered high-risk issues, agency Inspector General’s major management challenges, and other external and internal reviews in developing its reform efforts?
		Are the agency’s efforts to address those challenges consistent with the proven approach GAO has found to resolve high-risk issues? Agencies can show progress by addressing our five criteria for removal from the High-Risk List: leadership commitment, capacity, action plan, monitoring, and demonstrated progress. The five criteria form a road map for efforts to improve and ultimately address high-risk issues.
		How has the agency identified and addressed critical management challenges in areas such as information technology, cybersecurity, acquisition management, and financial management that can assist in the reform process?
		How does the agency plan to monitor the effects proposed reforms will have on high-risk areas?
		Has the agency addressed ways to decrease the risk of fraud, waste, and abuse of programs as part of its proposed reforms?
		How have findings and open recommendations from GAO and the agency Inspectors General been addressed in the proposed reform?

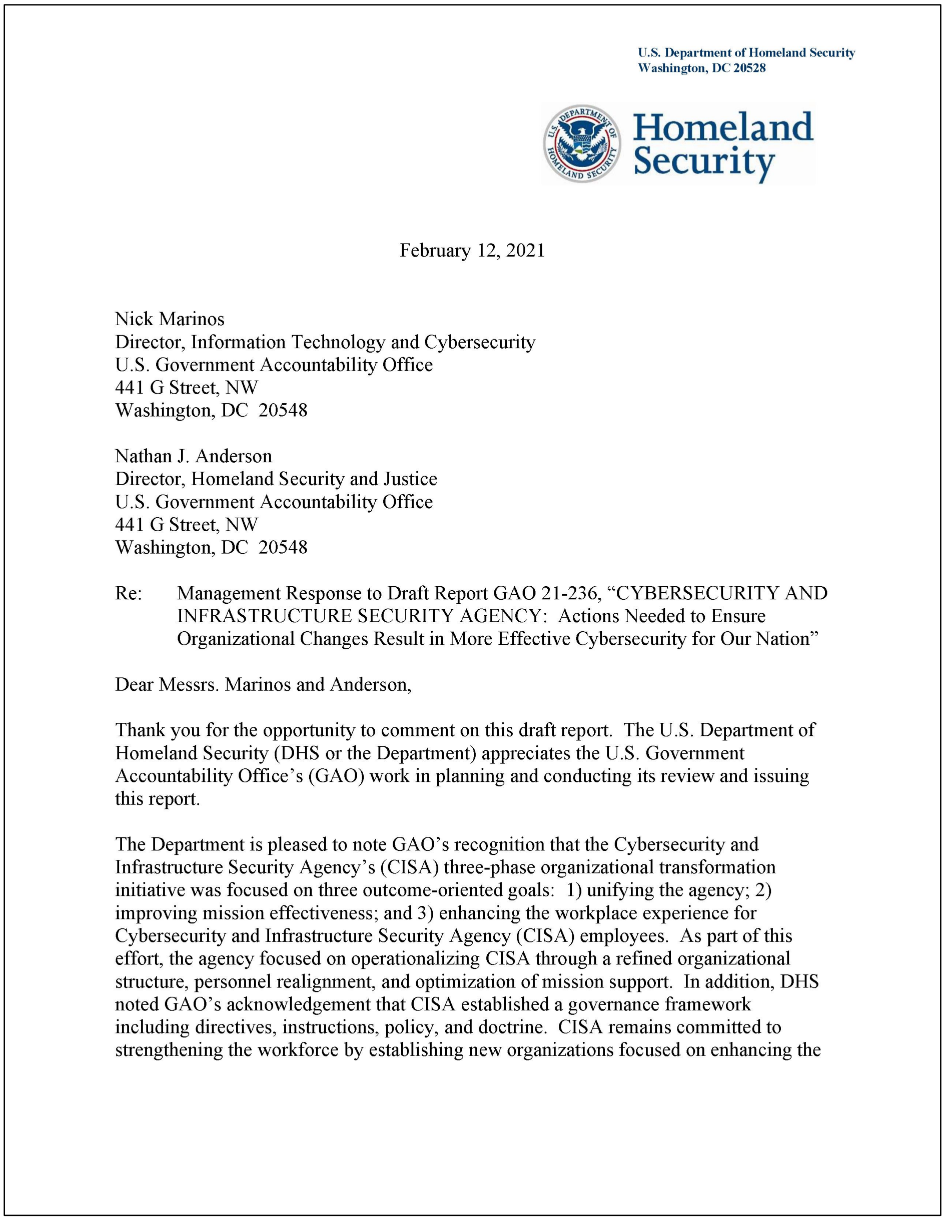
Category	Subcategory	Key questions
		How has the agency addressed GAO's priority open recommendations, which are those that warrant priority attention from heads of key departments and agencies?
Implementing reforms	Ensuring leadership focus and attention	Has the agency designated a leader or leaders to be responsible for the implementation of the proposed reforms?
		Has agency leadership defined and articulated a succinct and compelling reason for the reforms (i.e. a case for change)?
		How will the agency hold the leader or leaders accountable for successful implementation of the reforms?
		Has the agency established a dedicated implementation team that has the capacity, including staffing, resources, and change management, to manage the reform process?
	Managing and monitoring	How has the agency ensured their continued delivery of services during reform implementation?
		What implementation goals and a timeline have been set to build momentum and show progress for the reforms? In other words, has the agency developed an implementation plan with key milestones and deliverables to track implementation progress?
		How is the agency ensuring transparency over the progress of its reform efforts through web-based reporting on key milestones?
		Has the agency put processes in place to collect the needed data and evidence that will effectively measure the reform's outcome-oriented goals?
		How is the agency planning to measure customer satisfaction with the changes resulting from its reforms?
Strategically managing the federal workforce	Strengthening employee engagement	What do Federal Employee Viewpoint Survey results show for the agency's current employee engagement status both overall and disaggregated to lower organizational levels?
		How does the agency plan to sustain and strengthen employee engagement during and after the reforms?
		How specifically is the agency planning to manage diversity and ensure an inclusive work environment in its reforms, or as it considers workforce reductions?
	Conducting strategic workforce planning	To what extent has the agency conducted strategic workforce planning to determine whether it will have the needed resources and capacity, including the skills and competencies, in place for the proposed reforms or reorganization?
		How has the agency assessed the effects of the proposed agency reforms on the current and future workforce and what does that assessment show?
		To what extent does the agency track the number and cost of contractors supporting its agency mission and the functions those contractors are performing?
		How has the agency ensured that actions planned to maintain productivity and service levels do not cost more than the savings generated by reducing the workforce?

Category	Subcategory	Key questions
		What succession planning has the agency developed and implemented for leadership and other key positions in areas critical to reforms and mission accomplishment?
		To what extent have reforms included important practices for effective recruitment and hiring such as customized strategies to recruit highly specialized and hard-to-fill positions?
		What employment- and mission-related data has the agency identified to monitor progress of reform efforts and to ensure no adverse impact on agency mission, and how is it using that data?
	Ensuring effective employee performance management	To what extent has the agency aligned its employee performance management system with its planned reform goals?
		How has the agency included accountability for proposed change implementation in the performance expectations and assessments of leadership and staff at all levels?
		As part of the proposed reform development process, to what extent has the agency assessed its performance management to ensure it creates incentives for and rewards top performers, while ensuring it deals with poor performers?
		To what extent is the agency taking action to deal with employees with unacceptable performance and increasing the use of alternative dispute resolution to address workplace disputes that involve disciplinary or adverse actions?

Source: GAO. | GAO-21-236

Note: Questions are from GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

Appendix IV: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

February 12, 2021

Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

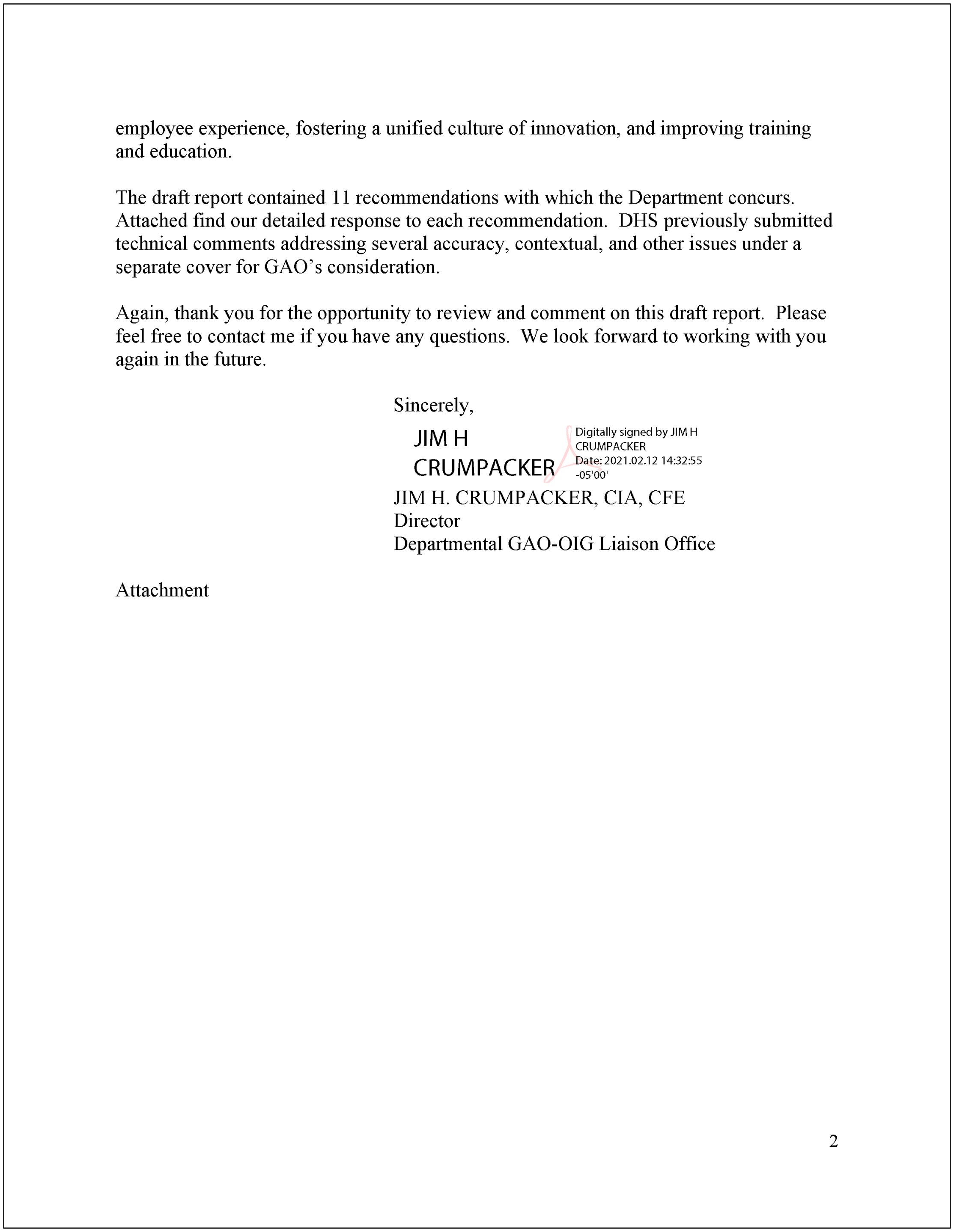
Nathan J. Anderson
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO 21-236, "CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation"

Dear Messrs. Marinos and Anderson,

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that the Cybersecurity and Infrastructure Security Agency's (CISA) three-phase organizational transformation initiative was focused on three outcome-oriented goals: 1) unifying the agency; 2) improving mission effectiveness; and 3) enhancing the workplace experience for Cybersecurity and Infrastructure Security Agency (CISA) employees. As part of this effort, the agency focused on operationalizing CISA through a refined organizational structure, personnel realignment, and optimization of mission support. In addition, DHS noted GAO's acknowledgement that CISA established a governance framework including directives, instructions, policy, and doctrine. CISA remains committed to strengthening the workforce by establishing new organizations focused on enhancing the



employee experience, fostering a unified culture of innovation, and improving training and education.

The draft report contained 11 recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

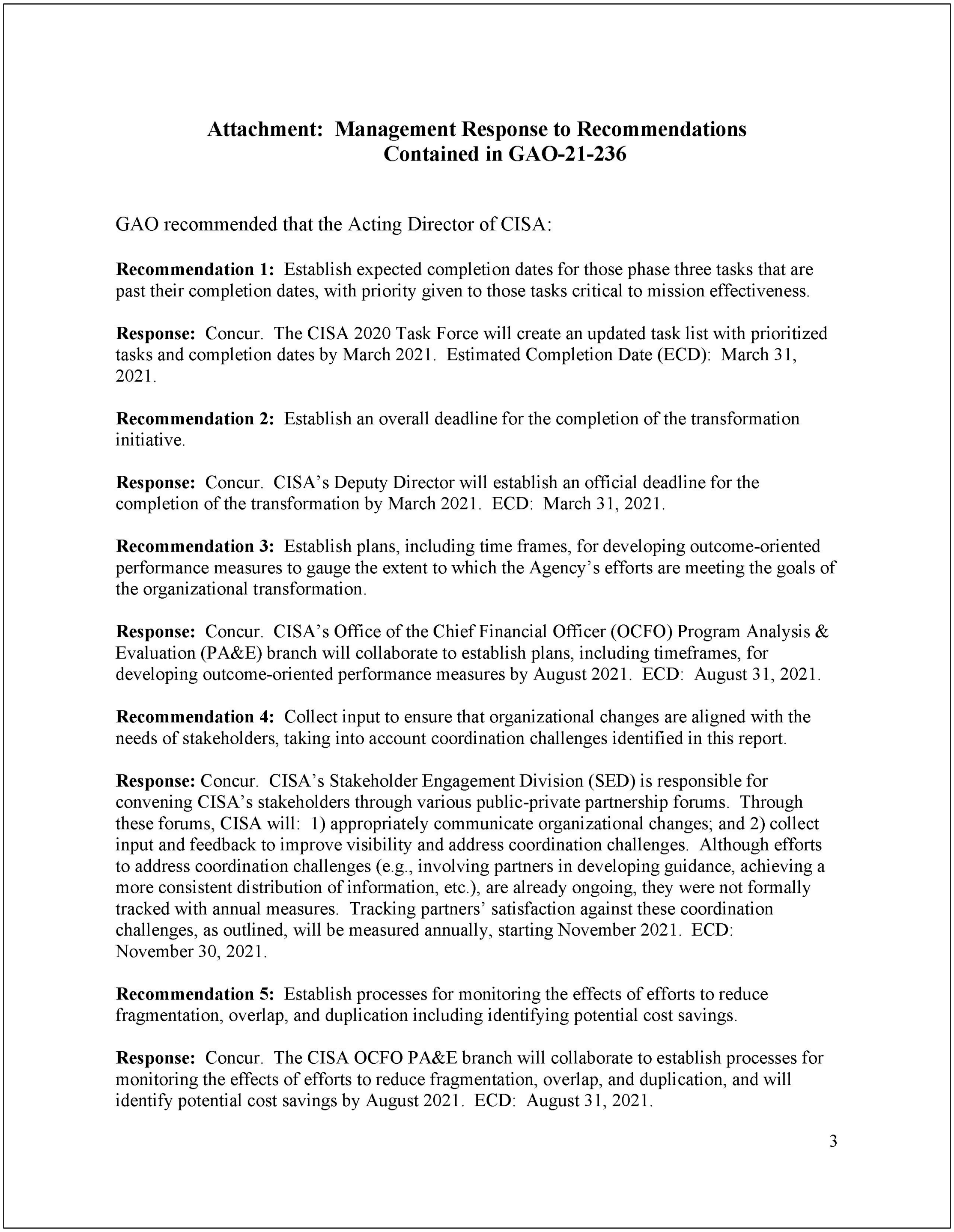
Sincerely,

JIM H
CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2021.02.12 14:32:55
-05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment



Attachment: Management Response to Recommendations Contained in GAO-21-236

GAO recommended that the Acting Director of CISA:

Recommendation 1: Establish expected completion dates for those phase three tasks that are past their completion dates, with priority given to those tasks critical to mission effectiveness.

Response: Concur. The CISA 2020 Task Force will create an updated task list with prioritized tasks and completion dates by March 2021. Estimated Completion Date (ECD): March 31, 2021.

Recommendation 2: Establish an overall deadline for the completion of the transformation initiative.

Response: Concur. CISA's Deputy Director will establish an official deadline for the completion of the transformation by March 2021. ECD: March 31, 2021.

Recommendation 3: Establish plans, including time frames, for developing outcome-oriented performance measures to gauge the extent to which the Agency's efforts are meeting the goals of the organizational transformation.

Response: Concur. CISA's Office of the Chief Financial Officer (OCFO) Program Analysis & Evaluation (PA&E) branch will collaborate to establish plans, including timeframes, for developing outcome-oriented performance measures by August 2021. ECD: August 31, 2021.

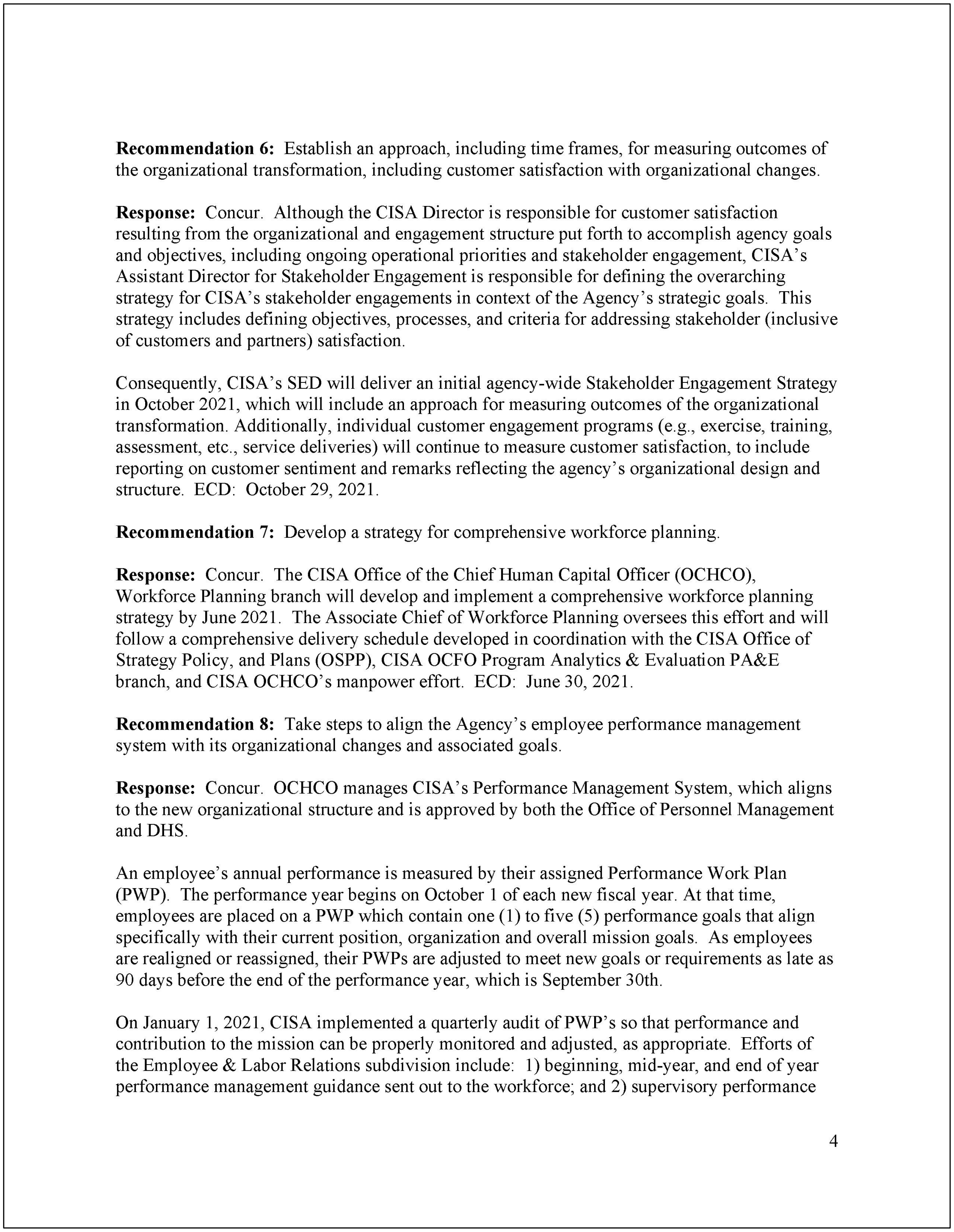
Recommendation 4: Collect input to ensure that organizational changes are aligned with the needs of stakeholders, taking into account coordination challenges identified in this report.

Response: Concur. CISA's Stakeholder Engagement Division (SED) is responsible for convening CISA's stakeholders through various public-private partnership forums. Through these forums, CISA will: 1) appropriately communicate organizational changes; and 2) collect input and feedback to improve visibility and address coordination challenges. Although efforts to address coordination challenges (e.g., involving partners in developing guidance, achieving a more consistent distribution of information, etc.), are already ongoing, they were not formally tracked with annual measures. Tracking partners' satisfaction against these coordination challenges, as outlined, will be measured annually, starting November 2021. ECD: November 30, 2021.

Recommendation 5: Establish processes for monitoring the effects of efforts to reduce fragmentation, overlap, and duplication including identifying potential cost savings.

Response: Concur. The CISA OCFO PA&E branch will collaborate to establish processes for monitoring the effects of efforts to reduce fragmentation, overlap, and duplication, and will identify potential cost savings by August 2021. ECD: August 31, 2021.

3



Recommendation 6: Establish an approach, including time frames, for measuring outcomes of the organizational transformation, including customer satisfaction with organizational changes.

Response: Concur. Although the CISA Director is responsible for customer satisfaction resulting from the organizational and engagement structure put forth to accomplish agency goals and objectives, including ongoing operational priorities and stakeholder engagement, CISA's Assistant Director for Stakeholder Engagement is responsible for defining the overarching strategy for CISA's stakeholder engagements in context of the Agency's strategic goals. This strategy includes defining objectives, processes, and criteria for addressing stakeholder (inclusive of customers and partners) satisfaction.

Consequently, CISA's SED will deliver an initial agency-wide Stakeholder Engagement Strategy in October 2021, which will include an approach for measuring outcomes of the organizational transformation. Additionally, individual customer engagement programs (e.g., exercise, training, assessment, etc., service deliveries) will continue to measure customer satisfaction, to include reporting on customer sentiment and remarks reflecting the agency's organizational design and structure. ECD: October 29, 2021.

Recommendation 7: Develop a strategy for comprehensive workforce planning.

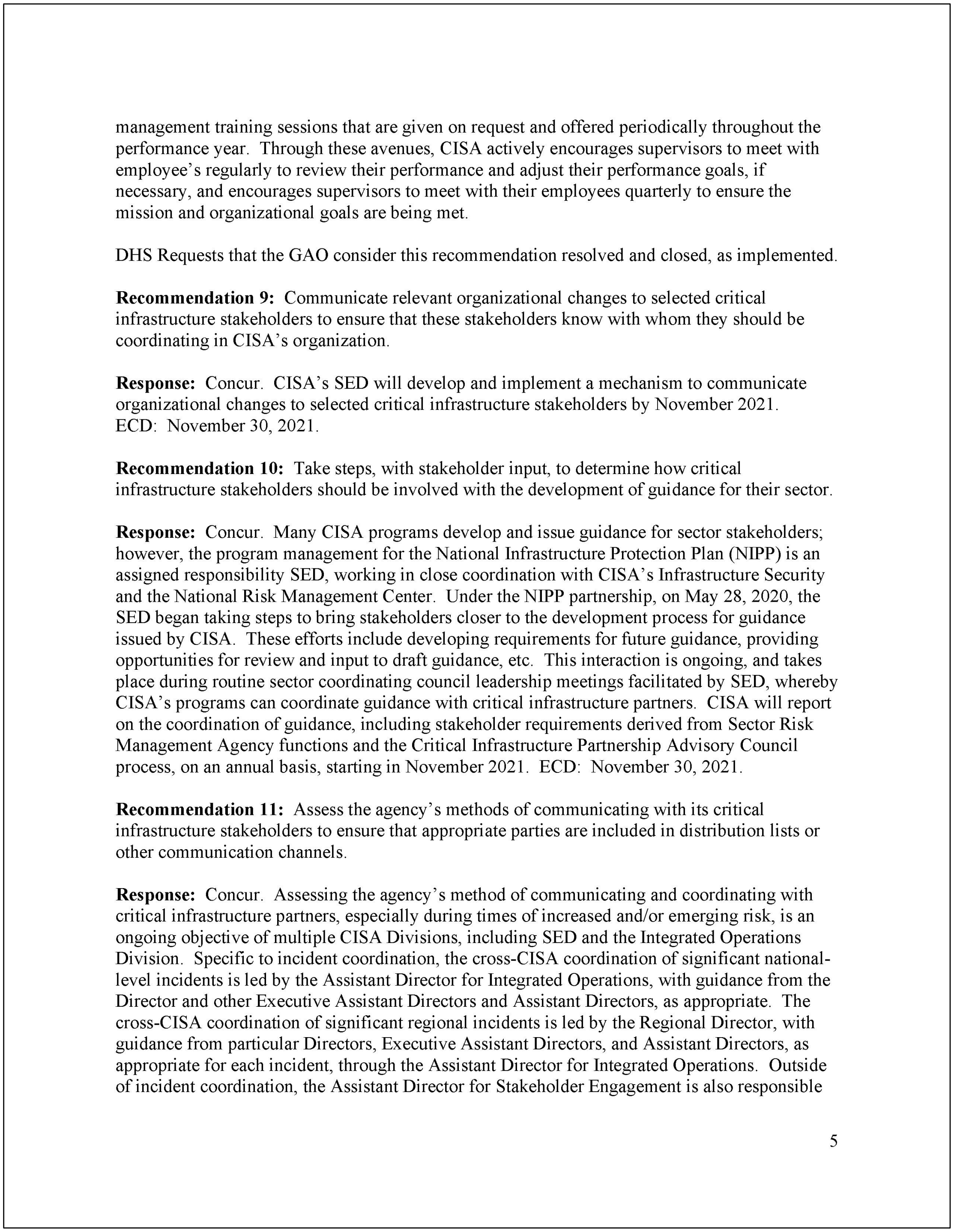
Response: Concur. The CISA Office of the Chief Human Capital Officer (OCHCO), Workforce Planning branch will develop and implement a comprehensive workforce planning strategy by June 2021. The Associate Chief of Workforce Planning oversees this effort and will follow a comprehensive delivery schedule developed in coordination with the CISA Office of Strategy Policy, and Plans (OSPP), CISA OCFO Program Analytics & Evaluation PA&E branch, and CISA OCHCO's manpower effort. ECD: June 30, 2021.

Recommendation 8: Take steps to align the Agency's employee performance management system with its organizational changes and associated goals.

Response: Concur. OCHCO manages CISA's Performance Management System, which aligns to the new organizational structure and is approved by both the Office of Personnel Management and DHS.

An employee's annual performance is measured by their assigned Performance Work Plan (PWP). The performance year begins on October 1 of each new fiscal year. At that time, employees are placed on a PWP which contain one (1) to five (5) performance goals that align specifically with their current position, organization and overall mission goals. As employees are realigned or reassigned, their PWPs are adjusted to meet new goals or requirements as late as 90 days before the end of the performance year, which is September 30th.

On January 1, 2021, CISA implemented a quarterly audit of PWP's so that performance and contribution to the mission can be properly monitored and adjusted, as appropriate. Efforts of the Employee & Labor Relations subdivision include: 1) beginning, mid-year, and end of year performance management guidance sent out to the workforce; and 2) supervisory performance



management training sessions that are given on request and offered periodically throughout the performance year. Through these avenues, CISA actively encourages supervisors to meet with employee's regularly to review their performance and adjust their performance goals, if necessary, and encourages supervisors to meet with their employees quarterly to ensure the mission and organizational goals are being met.

DHS Requests that the GAO consider this recommendation resolved and closed, as implemented.

Recommendation 9: Communicate relevant organizational changes to selected critical infrastructure stakeholders to ensure that these stakeholders know with whom they should be coordinating in CISA's organization.

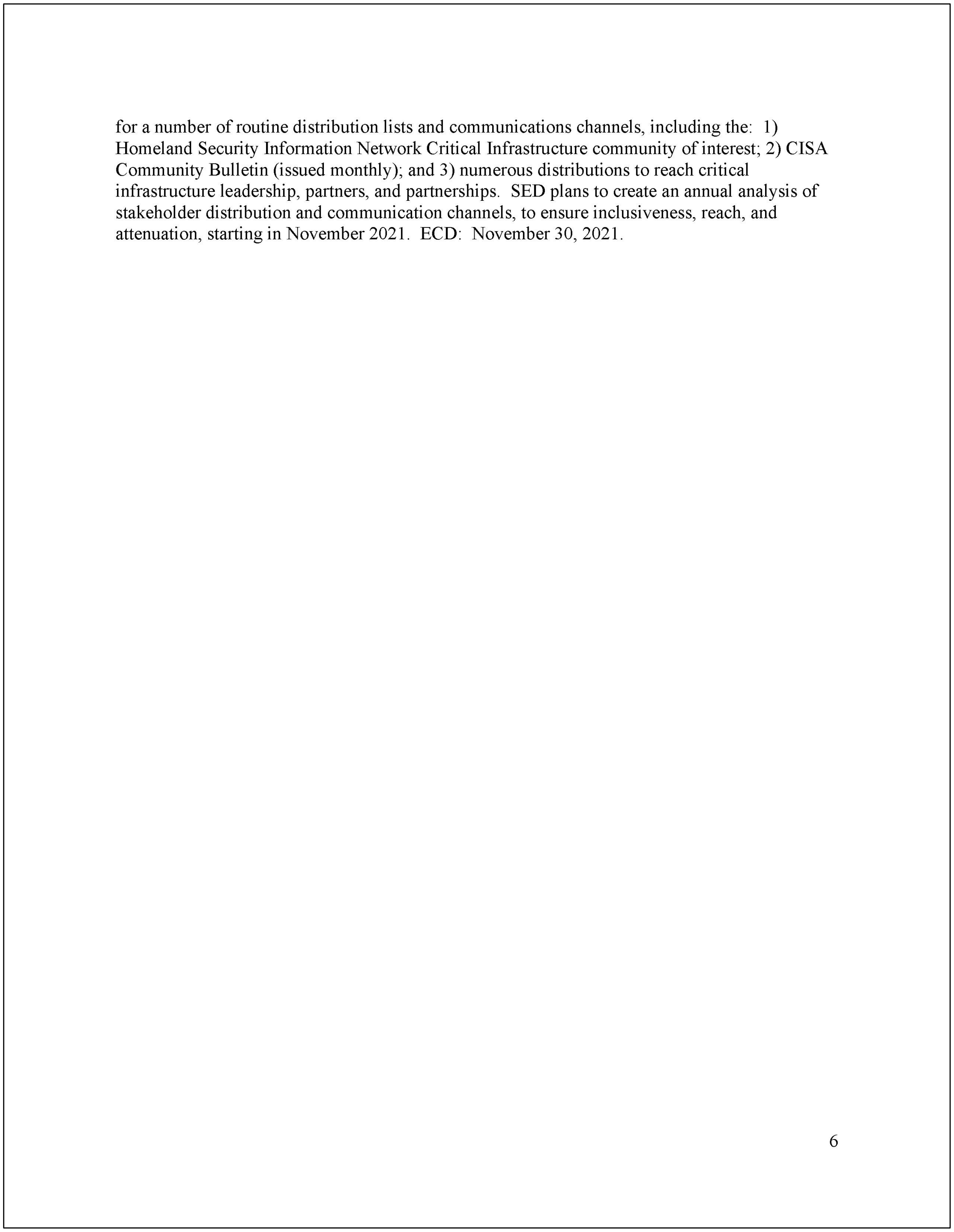
Response: Concur. CISA's SED will develop and implement a mechanism to communicate organizational changes to selected critical infrastructure stakeholders by November 2021.
ECD: November 30, 2021.

Recommendation 10: Take steps, with stakeholder input, to determine how critical infrastructure stakeholders should be involved with the development of guidance for their sector.

Response: Concur. Many CISA programs develop and issue guidance for sector stakeholders; however, the program management for the National Infrastructure Protection Plan (NIPP) is an assigned responsibility SED, working in close coordination with CISA's Infrastructure Security and the National Risk Management Center. Under the NIPP partnership, on May 28, 2020, the SED began taking steps to bring stakeholders closer to the development process for guidance issued by CISA. These efforts include developing requirements for future guidance, providing opportunities for review and input to draft guidance, etc. This interaction is ongoing, and takes place during routine sector coordinating council leadership meetings facilitated by SED, whereby CISA's programs can coordinate guidance with critical infrastructure partners. CISA will report on the coordination of guidance, including stakeholder requirements derived from Sector Risk Management Agency functions and the Critical Infrastructure Partnership Advisory Council process, on an annual basis, starting in November 2021. ECD: November 30, 2021.

Recommendation 11: Assess the agency's methods of communicating with its critical infrastructure stakeholders to ensure that appropriate parties are included in distribution lists or other communication channels.

Response: Concur. Assessing the agency's method of communicating and coordinating with critical infrastructure partners, especially during times of increased and/or emerging risk, is an ongoing objective of multiple CISA Divisions, including SED and the Integrated Operations Division. Specific to incident coordination, the cross-CISA coordination of significant national-level incidents is led by the Assistant Director for Integrated Operations, with guidance from the Director and other Executive Assistant Directors and Assistant Directors, as appropriate. The cross-CISA coordination of significant regional incidents is led by the Regional Director, with guidance from particular Directors, Executive Assistant Directors, and Assistant Directors, as appropriate for each incident, through the Assistant Director for Integrated Operations. Outside of incident coordination, the Assistant Director for Stakeholder Engagement is also responsible



for a number of routine distribution lists and communications channels, including the: 1) Homeland Security Information Network Critical Infrastructure community of interest; 2) CISA Community Bulletin (issued monthly); and 3) numerous distributions to reach critical infrastructure leadership, partners, and partnerships. SED plans to create an annual analysis of stakeholder distribution and communication channels, to ensure inclusiveness, reach, and attenuation, starting in November 2021. ECD: November 30, 2021.

Text of Appendix IV: Comments from the Department of Homeland Security

Page 1

February 12, 2021

Nick Marinos

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Nathan J. Anderson

Director, Homeland Security and Justice

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO 21-236, "CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation"

Dear Messrs. Marinos and Anderson,

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that the Cybersecurity and Infrastructure Security Agency's (CISA) three-phase organizational transformation initiative was focused on three outcome-oriented goals: 1) unifying the agency; 2) improving mission effectiveness; and 3) enhancing the workplace experience for Cybersecurity and Infrastructure Security Agency (CISA) employees. As part of this effort, the agency focused on operationalizing CISA through a refined organizational structure, personnel realignment, and optimization of mission support. In addition, DHS noted GAO's acknowledgement that CISA established a governance framework including directives, instructions, policy, and doctrine. CISA remains committed to strengthening the workforce by establishing new organizations focused on enhancing the

Page 2

employee experience, fostering a unified culture of innovation, and improving training and education.

The draft report contained 11 recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GAO-21-236

GAO recommended that the Acting Director of CISA:

Recommendation 1: Establish expected completion dates for those phase three tasks that are past their completion dates, with priority given to those tasks critical to mission effectiveness.

Response: Concur. The CISA 2020 Task Force will create an updated task list with prioritized tasks and completion dates by March 2021. Estimated Completion Date (ECD): March 31, 2021.

Recommendation 2: Establish an overall deadline for the completion of the transformation initiative.

Response: Concur. CISA's Deputy Director will establish an official deadline for the completion of the transformation by March 2021. ECD: March 31, 2021.

Recommendation 3: Establish plans, including time frames, for developing outcome-oriented performance measures to gauge the extent to which the Agency's efforts are meeting the goals of the organizational transformation.

Response: Concur. CISA's Office of the Chief Financial Officer (OCFO) Program Analysis & Evaluation (PA&E) branch will collaborate to establish plans, including timeframes, for developing outcome-oriented performance measures by August 2021. ECD: August 31, 2021.

Recommendation 4: Collect input to ensure that organizational changes are aligned with the needs of stakeholders, taking into account coordination challenges identified in this report.

Response: Concur. CISA's Stakeholder Engagement Division (SED) is responsible for convening CISA's stakeholders through various public-private partnership forums. Through these forums, CISA will: 1) appropriately communicate organizational changes; and 2) collect input and feedback to improve visibility and address coordination challenges. Although efforts to address coordination challenges (e.g., involving partners in developing guidance, achieving a more consistent distribution of information, etc.), are already ongoing, they were not formally tracked with annual measures. Tracking partners' satisfaction against these coordination challenges, as outlined, will be measured annually, starting November 2021. ECD:

November 30, 2021.

Recommendation 5: Establish processes for monitoring the effects of efforts to reduce fragmentation, overlap, and duplication including identifying potential cost savings.

Response: Concur. The CISA OCFO PA&E branch will collaborate to establish processes for monitoring the effects of efforts to reduce fragmentation, overlap, and duplication, and will identify potential cost savings by August 2021. ECD: August 31, 2021.

Page 4

Recommendation 6: Establish an approach, including time frames, for measuring outcomes of the organizational transformation, including customer satisfaction with organizational changes.

Response: Concur. Although the CISA Director is responsible for customer satisfaction resulting from the organizational and engagement structure put forth to accomplish agency goals and objectives, including ongoing operational priorities and stakeholder engagement, CISA's Assistant Director for Stakeholder Engagement is responsible for defining the overarching strategy for CISA's stakeholder engagements in context of the Agency's strategic goals. This strategy includes defining objectives, processes, and criteria for addressing stakeholder (inclusive of customers and partners) satisfaction.

Consequently, CISA's SED will deliver an initial agency-wide Stakeholder Engagement Strategy in October 2021, which will include an approach for measuring outcomes of the organizational transformation. Additionally, individual customer engagement programs (e.g., exercise, training, assessment, etc., service deliveries) will continue to measure customer satisfaction, to include reporting on customer sentiment and remarks reflecting the agency's organizational design and structure. ECD: October 29, 2021.

Recommendation 7: Develop a strategy for comprehensive workforce planning.

Response: Concur. The CISA Office of the Chief Human Capital Officer (OCHCO), Workforce Planning branch will develop and implement a comprehensive workforce planning strategy by June 2021. The Associate Chief of Workforce Planning oversees this effort and will follow a comprehensive delivery schedule developed in coordination with the CISA Office of Strategy Policy, and Plans (OSPP), CISA OCFO Program Analytics &

Evaluation PA&E branch, and CISA OCHCO's manpower effort. ECD: June 30, 2021.

Recommendation 8: Take steps to align the Agency's employee performance management system with its organizational changes and associated goals.

Response: Concur. OCHCO manages CISA's Performance Management System, which aligns to the new organizational structure and is approved by both the Office of Personnel Management and DHS.

An employee's annual performance is measured by their assigned Performance Work Plan (PWP). The performance year begins on October 1 of each new fiscal year. At that time, employees are placed on a PWP which contain one (1) to five (5) performance goals that align specifically with their current position, organization and overall mission goals. As employees are realigned or reassigned, their PWPs are adjusted to meet new goals or requirements as late as 90 days before the end of the performance year, which is September 30th.

On January 1, 2021, CISA implemented a quarterly audit of PWP's so that performance and contribution to the mission can be properly monitored and adjusted, as appropriate. Efforts of the Employee & Labor Relations subdivision include: 1) beginning, mid-year, and end of year performance management guidance sent out to the workforce; and 2) supervisory performance

Page 5

management training sessions that are given on request and offered periodically throughout the performance year. Through these avenues, CISA actively encourages supervisors to meet with employee's regularly to review their performance and adjust their performance goals, if necessary, and encourages supervisors to meet with their employees quarterly to ensure the mission and organizational goals are being met.

DHS Requests that the GAO consider this recommendation resolved and closed, as implemented.

Recommendation 9: Communicate relevant organizational changes to selected critical infrastructure stakeholders to ensure that these stakeholders know with whom they should be coordinating in CISA's organization.

Response: Concur. CISA's SED will develop and implement a mechanism to communicate organizational changes to selected critical infrastructure stakeholders by November 2021.

ECD: November 30, 2021.

Recommendation 10: Take steps, with stakeholder input, to determine how critical infrastructure stakeholders should be involved with the development of guidance for their sector.

**Response: Concur. Many CISA programs develop and issue guidance for sector stakeholders; however, the program management for the National Infrastructure Protection Plan (NIPP) is an assigned responsibility SED, working in close coordination with CISA's Infrastructure Security and the National Risk Management Center. Under the NIPP partnership, on May 28, 2020, the SED began taking steps to bring stakeholders closer to the development process for guidance issued by CISA. These efforts include developing requirements for future guidance, providing opportunities for review and input to draft guidance, etc. This interaction is ongoing, and takes place during routine sector coordinating council leadership meetings facilitated by SED, whereby CISA's programs can coordinate guidance with critical infrastructure partners. CISA will report on the coordination of guidance, including stakeholder requirements derived from Sector Risk Management Agency functions and the Critical Infrastructure Partnership Advisory Council process, on an annual basis, starting in November 2021.
ECD: November 30, 2021.**

Recommendation 11: Assess the agency's methods of communicating with its critical infrastructure stakeholders to ensure that appropriate parties are included in distribution lists or other communication channels.

Response: Concur. Assessing the agency's method of communicating and coordinating with critical infrastructure partners, especially during times of increased and/or emerging risk, is an ongoing objective of multiple CISA Divisions, including SED and the Integrated Operations Division. Specific to incident coordination, the cross-CISA coordination of significant national-level incidents is led by the Assistant Director for Integrated Operations, with guidance from the Director and other Executive Assistant Directors and Assistant Directors, as appropriate. The cross-CISA coordination of significant regional incidents is led by the Regional Director, with guidance from

particular Directors, Executive Assistant Directors, and Assistant Directors, as appropriate for each incident, through the Assistant Director for Integrated Operations. Outside of incident coordination, the Assistant Director for Stakeholder Engagement is also responsible

Page 6

for a number of routine distribution lists and communications channels, including the: 1) Homeland Security Information Network Critical Infrastructure community of interest; 2) CISA Community Bulletin (issued monthly); and 3) numerous distributions to reach critical infrastructure leadership, partners, and partnerships. SED plans to create an annual analysis of stakeholder distribution and communication channels, to ensure inclusiveness, reach, and attenuation, starting in November 2021. ECD: November 30, 2021.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342, marinosn@gao.gov

Nathan J. Anderson, (206) 287-4804, andersonn@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Marisol Cruz Cain (assistant director), Ben Atwater (assistant director), Lee McCracken (analyst in charge), Amy Apostol, Kiana Beshir, Chris Businsky, Tahj Clemons, David Dornisch, Donna Epler, Becca Eyler, Ryan Lester, Gabriel Nelson, Andrew Stavisky, and Sarah Veale.

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

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