United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. ET
Wednesday, March 6, 2019

# HIGH-RISK SERIES

# Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas

Statement of Gene L. Dodaro,
Comptroller General of the United States

March 2019

# HIGH-RISK SERIES

## Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas

GAO Highlights

Highlights of GAO-19-393T, a statement before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

The federal government is one of the world's largest and most complex entities; about $4.1 trillion in outlays in fiscal year 2018 funded a broad array of programs and operations. GAO's high-risk program identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation to address economy, efficiency, or effectiveness challenges.

This biennial update describes the status of high-risk areas, outlines actions that are still needed to assure further progress, and identifies two new high-risk areas needing attention by the executive branch and Congress. Solutions to high-risk problems save billions of dollars, improve service to the public, and would strengthen government performance and accountability.

GAO uses five criteria to assess progress in addressing high-risk areas: (1) leadership commitment, (2) agency capacity, (3) an action plan, (4) monitoring efforts, and (5) demonstrated progress.

## What GAO Recommends

This statement describes GAO's views on progress made and what remains to be done to bring about lasting solutions for each high-risk area. Substantial efforts are needed by the executive branch to achieve progress on high-risk areas. Addressing GAO's hundreds of open recommendations across the high-risk areas and continued congressional oversight and action are essential to achieving greater progress.

View GAO-19-393T. For more information, contact J. Christopher Mihm at (202) 512-6806 or mihmj@gao.gov.

## What GAO Found

The ratings for more than half of the 35 areas on the 2019 High-Risk List remain largely unchanged. Since GAO's last update in 2017, seven areas improved, three regressed, and two showed mixed progress by improving in some criteria but declining in others. Where there has been improvement in high-risk areas, congressional actions have been critical in spurring progress in addition to actions by executive agencies.

GAO is removing two of the seven areas with improved ratings from the High-Risk List because they met all of GAO's five criteria for removal. The first area, Department of Defense (DOD) Supply Chain Management, made progress on seven actions and outcomes related to monitoring and demonstrated progress that GAO recommended for improving supply chain management. For example, DOD improved the visibility of physical inventories, receipt processing, cargo tracking, and unit moves. Improvements in asset visibility have saved millions of dollars and allow DOD to better meet mission needs by providing assets where and when needed.

The second area, Mitigating Gaps in Weather Satellite Data, made significant progress in establishing and implementing plans to mitigate potential gaps. For example, the National Oceanic and Atmospheric Administration successfully launched a satellite, now called NOAA-20, in November 2017. NOAA-20 is operational and provides advanced weather data and forecasts. DOD developed plans and has taken actions to address gaps in weather data through its plans to launch the Weather System Follow-on–Microwave satellite in 2022.

There are two new areas on the High-Risk List since 2017. Added in 2018 outside of GAO's biennial high-risk update cycle, the Government-Wide Personnel Security Clearance Process faces significant challenges related to processing clearances in a timely fashion, measuring investigation quality, and ensuring information technology security. The second area, added in 2019, is Department of Veterans Affairs (VA) Acquisition Management. VA has one of the most significant acquisition functions in the federal government, both in obligations and number of contract actions. GAO identified seven contracting challenges for VA, such as outdated acquisition regulations and policies, lack of an effective medical supplies procurement strategy, and inadequate acquisition training.

Overall, 24 high-risk areas have either met or partially met all five criteria for removal from the list; 20 of these areas fully met at least one criterion. Ten high-risk areas have neither met nor partially met one or more criteria.

While progress is needed across all high-risk areas, GAO has identified nine that need especially focused executive and congressional attention, including Ensuring the Cybersecurity of the Nation, Resolving the Federal Role in Housing Finance, addressing Pension Benefit Guaranty Corporation Insurance Programs, Managing Risks and Improving VA Health Care, and ensuring an effective 2020 Decennial Census. Beyond these specific areas, focused attention is needed to address mission-critical skills gaps in 16 high-risk areas, confront three high-risk areas concerning health care and tax law enforcement that include billions of dollars in improper payments each year, and focus on a yawning tax gap.

**GAO's 2019 High-Risk List**

| |
|---|
| **Strengthening the Foundation for Efficiency and Effectiveness** |
| Strategic Human Capital Management |
| Managing Federal Real Property |
| Funding the Nation's Surface Transportation System[a] |
| Modernizing the U.S. Financial Regulatory System[a] |
| Resolving the Federal Role in Housing Finance[a] |
| USPS Financial Viability[a] |
| Management of Federal Oil and Gas Resources |
| Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks[a] |
| Improving the Management of IT Acquisitions and Operations |
| Improving Federal Management of Programs That Serve Tribes and Their Members[a] |
| 2020 Decennial Census[a] |
| U.S. Government Environmental Liability[a] |
| **Transforming DOD Program Management** |
| DOD Weapon Systems Acquisition |
| DOD Financial Management |
| DOD Business Systems Modernization |
| DOD Support Infrastructure Management[a] |
| DOD Approach to Business Transformation |
| **Ensuring Public Safety and Security** |
| Government-wide Personnel Security Clearance Process (new)[a] |
| Ensuring the Cybersecurity of the Nation[a] |
| Strengthening Department of Homeland Security Management Functions |
| Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests[a] |
| Improving Federal Oversight of Food Safety[a] |
| Protecting Public Health through Enhanced Oversight of Medical Products |
| Transforming EPA's Processes for Assessing and Controlling Toxic Chemicals[a] |
| **Managing Federal Contracting More Effectively** |
| VA Acquisition Management (new) |
| DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management[a] |
| NASA Acquisition Management[a] |
| DOD Contract Management |
| **Assessing the Efficiency and Effectiveness of Tax Law Administration** |
| Enforcement of Tax Laws[a] |
| **Modernizing and Safeguarding Insurance and Benefit Programs** |
| Medicare Program & Improper Payments[a] |
| Strengthening Medicaid Program Integrity[a] |
| Improving and Modernizing Federal Disability Programs |
| Pension Benefit Guaranty Corporation Insurance Programs[a] |
| National Flood Insurance Program[a] |
| Managing Risks and Improving VA Health Care[a] |

Source: GAO. | GAO-19-157SP

[a]Legislation is likely to be necessary in order to effectively address this area.

Chairman Johnson, Ranking Member Peters, and Members of the Committee:

Since the early 1990s, our high-risk program has focused attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement, or that are in need of transformation to address economy, efficiency, or effectiveness challenges. This effort, supported by this committee and the House of Representatives Committee on Oversight and Reform, has brought much needed attention to problems impeding effective government and costing billions of dollars each year.

We have made hundreds of recommendations to reduce the government's high-risk challenges. Executive agencies either have addressed or are addressing many of them and, as a result, progress is being made in a number of areas. Congress also continues to take important actions. For example, Congress has enacted a number of laws since our last report in February 2017 that are helping to make progress on high-risk issues. Financial benefits to the federal government due to progress in addressing high-risk areas over the past 13 years (fiscal year 2006 through fiscal year 2018) totaled nearly $350 billion or an average of about $27 billion per year. In fiscal year 2018, financial benefits were the highest we ever reported at nearly $47 billion.[1]

You asked me today to focus particularly on those high-risk areas that fall within the legislative jurisdiction of the Committee. Many of those are discussed throughout this statement. Appendix I contains the high-risk summaries for the following areas:

- Strategic Human Capital Management
- Managing Federal Real Property
- USPS Financial Viability
- Improving the Management of IT Acquisitions and Operations
- 2020 Decennial Census
- Government-wide Personnel Security Clearance Process
- Ensuring the Cybersecurity of the Nation
- Strengthening Department of Homeland Security Management Functions

Our 2019 High-Risk Report, which is being released today, describes (1) progress made addressing high-risk areas and the reasons for that

[1]Financial benefits are based on actions taken in response to our work, such as reducing government expenditures, increasing revenues, or reallocating funds to other areas.

progress, and (2) actions that are still needed.[2] It also identifies two new high-risk areas—Government-wide Personnel Security Clearance Process and Department of Veterans Affairs (VA) Acquisition Management, and two high-risk areas we removed from the list because they demonstrated sufficient progress in managing risk—Department of Defense (DOD) Supply Chain Management and Mitigating Gaps in Weather Satellite Data.[3]

Substantial efforts are needed on the remaining high-risk areas to achieve greater progress and to address regress in some areas since the last high-risk update in 2017. Continued congressional attention and executive branch leadership attention remain key to success.

## How We Rate High-Risk Areas

Our experience has shown that the key elements needed to make progress in high-risk areas are top-level attention by the administration and agency leaders grounded in the five criteria for removal from the High-Risk List, as well as any needed congressional action.[4] The five criteria for removal that we issued in November 2000 are as follows:

- **Leadership commitment.** Demonstrated strong commitment and top leadership support.
- **Capacity.** Agency has the capacity (i.e., people and resources) to resolve the risk(s).
- **Action plan.** A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.
- **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.

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

[3]Government-wide Personnel Security Clearance Process was added to the High-Risk List in January 2018.

[4]GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

- **Demonstrated progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

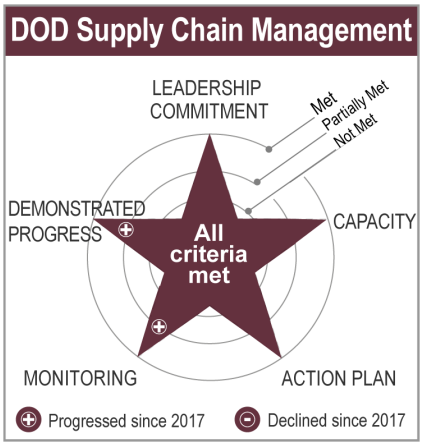
Starting in our 2015 update, we added clarity and specificity to our assessments by rating each high-risk area's progress on the five criteria and used the following definitions:

- **Met.** Actions have been taken that meet the criterion. There are no significant actions that need to be taken to further address this criterion.
- **Partially met.** Some, but not all, actions necessary to meet the criterion have been taken.
- **Not met.** Few, if any, actions towards meeting the criterion have been taken.

## Changes to the 2019 High-Risk List

We are removing two areas—DOD Supply Chain Management and Mitigating Gaps in Weather Satellite Data—from the list due to the progress that was made in addressing the high-risk issues. As we have with areas previously removed from the High-Risk List, we will continue to monitor these areas to ensure that the improvements we have noted are sustained. If significant problems again arise, we will consider reapplying the high-risk designation. We added two areas to the High-Risk List since our 2017 update—Government-Wide Personnel Security Clearance Process and VA Acquisition Management.

## DOD Supply Chain Management Removed From the High-Risk List




Source: GAO analysis. | GAO-19-157SP

We are removing the area of DOD Supply Chain Management from the High-Risk List because, since 2017, DOD has addressed the remaining two criteria (monitoring and demonstrated progress) for the asset visibility and materiel distribution segments. Congressional attention, DOD leadership commitment, and our collaboration contributed to the successful outcome for this high-risk area, which had been on GAO's High-Risk List since 1990.

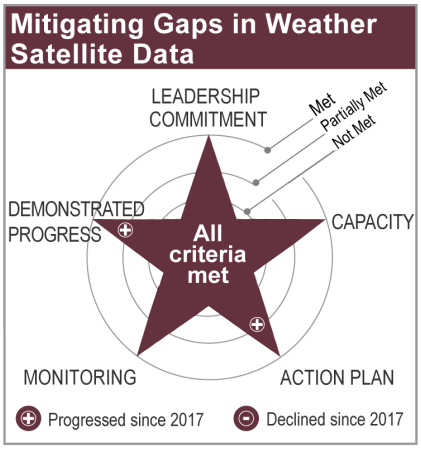
DOD's actions for the asset visibility segment of this high-risk area included (1) providing guidance for the military components to consider key attributes of successful performance measures during metric development for their improvement initiatives; (2) incorporating into after-action reports, information relating to performance measures; and (3) demonstrating sustained progress by, for example, increasing its visibility of assets through radio-frequency identification (RFID), an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. According to DOD, the use of RFID tags to provide visibility of sustainment cargo at the tactical leg (i.e., the last segment of the distribution system) resulted in $1.4 million annual cost savings.

DOD's actions for the materiel distribution segment of this high-risk area included (1) making progress in developing its suite of distribution performance metrics; (2) incorporating distribution metrics, as appropriate, on the performance of all legs of the distribution system, including the tactical leg; (3) making progress in refining its Materiel Distribution Improvement Plan and incorporating additional actions based on interim progress and results; and (4) improving its capability to comprehensively measure distribution performance, identifying distribution problems and root cause, and implementing solutions. According to DOD, initiatives focused on distribution process and operational improvements have resulted in at least $1.56 billion in distribution cost avoidances to date.

As we have with areas previously removed from the High-Risk List, we will continue to monitor this area to ensure that the improvements we have noted are sustained.[5] Appendix II provides additional information on this high-risk area.

[5]For additional details on the reasons for removing this high-risk area, see p. 102 of this statement.

## Mitigating Gaps in Weather Satellite Data Removed From the High-Risk List




Source: GAO analysis. | GAO-19-157SP

We are removing the area of Mitigating Gaps in Weather Satellite Data from the High-Risk List because—with strong congressional support and oversight—the National Oceanic and Atmospheric Administration (NOAA) and DOD have made significant progress since 2017 in establishing and implementing plans to mitigate potential gaps in weather satellite data.

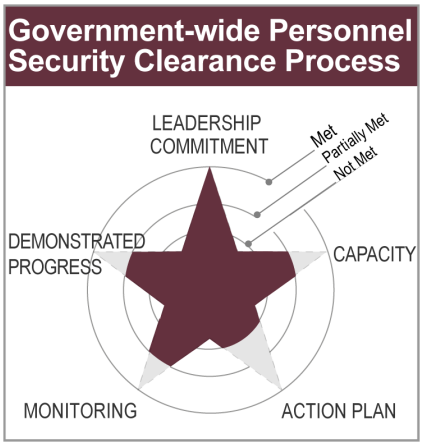
The United States relies on polar-orbiting satellites to provide a global perspective on weather every morning and afternoon. NOAA is responsible for the polar satellite program that crosses the equator in the afternoon while DOD is responsible for the polar satellite program that crosses the equator in the early morning orbit. NOAA's actions for polar-orbiting weather satellites that addressed the remaining criteria of action plan and demonstrated progress included (1) issuing three updates to its gap mitigation plan between January 2016 and February 2017 to address shortfalls we had identified previously; and (2) successfully launching the NOAA-20 satellite in November 2017, which is currently operational and is being used to provide advanced weather data and forecasts. Moreover, NOAA is also working to build and launch the next satellites in the polar satellite program.

DOD's actions for polar-orbiting weather satellites, pursuant to statutes and accompanying congressional direction, included DOD leadership (1) developing and implementing plans to acquire satellites as part of a family of systems to replace its aging legacy weather satellites, including awarding a contract for its Weather System Follow-on–Microwave program, planned for launch in 2022; (2) establishing plans to meet its highest-priority weather monitoring data collection needs that will not be covered by the Weather System Follow-on–Microwave program, including by acquiring and launching the Electro-Optical/Infrared Weather Systems satellite in 2024; and (3) monitoring the Weather System Follow-on-Microwave satellite program's progress toward addressing critical needs and assessing its operations and sustainment costs.

As we have with areas previously removed from the High-Risk List, we will continue to monitor this area to ensure that the improvements we have noted are sustained.[6] Appendix II provides additional information on this high-risk area.

[6]For additional details on the reasons for removing this high-risk area, see p. 109 of this statement.

## Government-wide Personnel Security Clearance Process Added to the High-Risk List




Source: GAO analysis. | GAO-19-157SP

Executive branch agencies are not meeting investigation timeliness objectives, and these processing delays have contributed to a significant backlog that the National Background Investigations Bureau (NBIB)—the agency responsible for personnel security clearance investigations—reported to be approximately 565,000 investigations as of February 2019. In addition, the executive branch has not finalized performance measures to ensure the quality of background investigations and some long-standing key reform initiatives remain incomplete. Further, information technology (IT) security concerns may delay planned milestones for the development of a new background investigation IT system.

We included the DOD program on our High-Risk List in 2005 and removed it in 2011 because of improvements in the timeliness of investigations and adjudications, and steps toward measuring the quality of the process. We put the government-wide personnel security clearance process on our High-Risk List in January 2018 because of significant challenges related to the timely processing of security clearances and completing the development of quality measures. In addition, thITe government's effort to reform the personnel security clearance process, starting with the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, has had mixed progress, and key reform efforts have not been implemented government-wide.[7] Since adding this area to the High-Risk List, the Security Clearance, Suitability, and Credentialing Performance Accountability Council (PAC), including its four principal members—the Deputy Director for Management of the Office of Management and Budget (OMB), the Director of National Intelligence (DNI); the Under Secretary of Defense for Intelligence; and the Director of the Office of Personnel Management (OPM)—have not fully met the five criteria for high-risk removal.

Several issues contribute to the risks facing the government-wide personnel security clearance process:

- **Clearance processing delays**. Executive branch agencies are not meeting most investigation timeliness objectives. The percentage of executive branch agencies meeting established timeliness objectives for initial secret clearances, initial top secret clearances, and periodic reinvestigations decreased each year from fiscal years 2012 through 2018. For example, 97 percent of the executive branch agencies we

[7]Pub. L. No. 108-458, 118 Stat. 3638 (2004).

reviewed did not meet the timeliness objectives for initial secret clearance investigations in fiscal year 2018.

- **Lack of quality measures.** While the executive branch has taken steps to establish government-wide performance measures for the quality of background investigations—including establishing quality assessment standards and a quality assessment reporting tool—it is unclear when this effort will be completed.
- **Security clearance reform delays.** The executive branch has reformed many parts of the personnel security clearance process—such as updating adjudicative guidelines to establish common adjudicative criteria for security clearances; however, some long-standing key initiatives remain incomplete—such as completing plans to fully implement and monitor continuous evaluation.
- **IT security.** DOD is responsible for developing a new system to support background investigation processes, and DOD officials expressed concerns about the security of connecting to OPM's legacy systems since a 2015 data breach compromised OPM's background investigation systems and files for 21.5 million individuals. As of December 2018, OPM has not fully taken action on our priority recommendations to update its security plans, evaluate its security control assessments, and implement additional training opportunities.

However, since we added this area to our High-Risk List, the PAC has demonstrated progress in some areas. For example, NBIB reported that the backlog of background investigations decreased from almost 715,000 cases in January 2018 to approximately 565,000 cases in February 2019. NBIB officials credit an Executive Memorandum—issued jointly in June 2018 by the DNI and the Director of OPM and containing measures to reduce the investigation backlog—as a driver in backlog reduction.

Further, in response to a requirement in the Securely Expediting Clearances Through Reporting Transparency (SECRET) Act of 2018, in September 2018, NBIB reported to Congress, for each clearance level, (1) the size of the investigation backlog, (2) the average length of time to conduct an initial investigation and a periodic reinvestigation, and (3) a discussion of the factors contributing to investigation timeliness.[8] The PAC is also reporting publicly on the progress of key reforms through www.performance.gov, and for fiscal year 2018, the website contains

[8]Pub. L. No. 115-173, § 3, 132 Stat. 1291, 1291–1292 (2018).

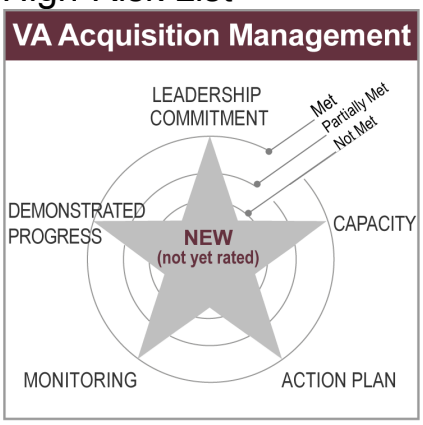
quarterly action plans and progress updates, which present figures on the average timeliness of initial investigations and periodic reinvestigations for the executive branch as a whole, investigation workload and backlog, and investigator headcounts.

We have made numerous recommendations to PAC members to address risks associated with the personnel security clearance process between 2011—when we removed DOD's personnel security clearance program from the High-Risk List, and 2018—when we placed the government-wide personnel security clearance process on the High-Risk List. We consider 27 of these recommendations key to addressing the high-risk designation. Eight recommendations key to the high-risk designation have been implemented, including three since January 2018.

Nineteen of these key recommendations remain open—including recommendations that the principal members of the PAC (1) conduct an evidence-based review of investigation and adjudication timeliness objectives, (2) develop and report to Congress on investigation quality measures, (3) prioritize the timely completion of efforts to modernize and secure IT systems that affect clearance holders government-wide, and (4) develop and implement a comprehensive workforce plan that identifies the workforce needed to meet current and future demand for background investigations services and to reduce the investigations backlog.

See page 170 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## VA Acquisition Management Added to the High-Risk List




Source: GAO analysis. | GAO-19-157SP

VA spends tens of billions of dollars to procure a wide range of goods and services—including medical supplies, IT, and construction of hospitals, clinics, and other facilities—to meet its mission of providing health care and other benefits to millions of veterans. VA has one of the most significant acquisition functions in the federal government, both in obligations and number of contract actions. The Veterans Health Administration (VHA) provides medical care to veterans and is by far the largest administration in the VA. Since we began focusing on VA's acquisition management activities in 2015, we have reported numerous challenges in this area. Since 2015, we have made 31 recommendations, 21 of which remain open, that cover a range of areas to address challenges in VA's acquisition management.

In fiscal year 2019, VA received the largest discretionary budget in its history—$86.5 billion, about $20 billion higher than in 2015. About a third of VA's discretionary budget in fiscal year 2017, or $26 billion, has been used to contract for goods and services. VA's acquisition management continues to face challenges including (1) outdated acquisition regulations and policies; (2) lack of an effective medical supplies procurement strategy; (3) inadequate acquisition training; (4) contracting officer workload challenges; (5) lack of reliable data systems; (6) limited contract oversight and incomplete contract file documentation; and (7) leadership instability.

In light of these challenges and given the significant taxpayer investment, it is imperative that VA show sustained leadership commitment to take steps to improve the performance of its procurement function so that it can use its funding in the most efficient manner possible to meet the needs of those who served our country.

This area has been added to the High-Risk List for the following reasons in particular:

- **Outdated acquisition regulations and policies.** VA's procurement policies have historically been outdated, disjointed, and difficult for contracting officers to use. In September 2016, we reported that the acquisition regulations contracting officers currently follow have not been fully updated since 2008 and that VA had been working on completing a comprehensive revision of its acquisition regulations since 2011. VA's delay in updating this fundamental source of policy has impeded the ability of contracting officers to effectively carry out their duties. We recommended in September 2016 that VA identify measures to expedite the revision of its acquisition regulations and

clarify what policies are currently in effect. VA concurred with this recommendation but has not yet fully implemented it.

- **Lack of an effective medical supplies procurement strategy.** VA's Medical Surgical Prime Vendor-Next Generation (MSPV-NG) program for purchasing medical supplies to meet the needs of about 9 million veterans at 172 medical centers has not been effectively executed, nor is it in line with practices at leading hospitals that have launched similar programs. We reported in November 2017 that VA's approach to developing its catalog of supplies was rushed and lacked key stakeholder involvement and buy-in. As a result, VA was not able to accomplish some of the key efficiencies the program was intended to achieve, such as streamlining the purchase of medical supplies and saving money. We recommended in November 2017 that VA develop, document, and communicate to stakeholders an overarching strategy for the program. VA concurred with this recommendation and reported that it would develop a new strategy by March 2019.
- **Contracting officer workload challenges**. The majority of our reviews since 2015 have highlighted workload as a contributing factor to the challenges that contracting officers face. Most recently, in September 2018, we reported that about 54 percent of surveyed VA contracting officers said their workload was not reasonable. In addition, in September 2016, we reported that VHA contracting officers processed a large number of emergency procurements of routine medical supplies, which accounted for approximately 20 percent of VHA's overall contract actions in fiscal year 2016, with obligations totaling about $1.9 billion.

Contracting officers told us that these frequent and urgent small-dollar transactions reduce contracting officers' efficiency and ability to take a strategic view of procurement needs. We recommended in November 2017 that VHA network contracting offices work with medical centers to identify opportunities to more strategically purchase goods and services frequently purchased on an emergency basis. VA concurred with this recommendation and reported in December 2018 that it is utilizing a supply chain dashboard to track items purchased on an emergency basis and determine which of those items to include on the catalog. VA noted that it added 13,300 items to the catalog from June 2018 to December 2018, including items often purchased on an emergency basis. We requested documentation showing which items added to the catalog were previously purchased on an emergency basis, but as of January 2019, VA had not yet provided it.

Among other things, VA should implement our 21 open recommendations and specifically needs to take the following steps to demonstrate greater leadership commitment and strategic planning to ensure efficient use of its acquisition funding and staffing resources:

- Prioritize completing the revision of its acquisition regulations, which has been in process since 2011.
- Develop, document, and communicate to stakeholders a strategy for the Medical Surgical Prime Vendor program to achieve overall program goals.
- Identify opportunities to strategically purchase goods and services that are frequently purchased on an emergency basis.

See page 210 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Emerging Issue Requiring Close Attention: Federal Efforts to Prevent Drug Misuse

In addition to specific areas that we have designated as high-risk, other important challenges facing our nation merit continuing close attention. One of these is the use of illicit drugs and the misuse of prescription drugs and the ways they affect individuals, their families, and the communities in which they live. Over 70,000 people died from drug overdoses in 2017—about 191 people every day—according to the Centers for Disease Control and Prevention, with the largest portion of these deaths attributed to opioids. Further, drug overdoses are the leading cause of death due to injuries in the United States. They are currently at their highest ever recorded level and, since 2011, have outnumbered deaths by firearms, motor vehicle crashes, suicide, and homicide, according to the Drug Enforcement Administration. The Council of Economic Advisors estimates that in 2015, the economic cost of the opioid crisis alone was more than $500 billion when considering the value of lives lost due to opioid-related overdose.

Federal drug control efforts spanning prevention, treatment, interdiction, international operations, and law enforcement represent a considerable federal investment. According to the President's fiscal year 2019 budget, federal drug control funding for fiscal year 2017 was $28.8 billion. Multiple federal agencies have ongoing efforts to respond to this crisis, including efforts to reduce the supply and demand for illicit drugs, to prevent misuse of prescription drugs, and to treat substance use disorders.

However, we previously found that many efforts lacked measures to gauge the success of the federal response. Further, we have long advocated an approach to decision-making based on risk management. Such an approach would (1) link agencies' plans and budgets to achieving their strategic goals, (2) assess values and risks of various courses of actions to help set priorities and allocate resources, and (3) provide for the use of performance measures to assess progress.

The Office of National Drug Control Policy (ONDCP) is responsible for overseeing and coordinating the implementation of U.S. drug policy, including developing the National Drug Control Strategy (Strategy). ONDCP released the 2019 Strategy on January 31, 2019. The Strategy focuses on approaches related to prevention, treatment and recovery, and steps to reduce the availability of illicit drugs in the United States. We will continue to monitor the extent to which ONDCP and other federal agencies are employing a risk management and coordinated approach to their efforts to limit drug misuse.

In particular, we have ongoing and planned work to assess ONDCP's operations, including its (1) leadership and coordination of efforts across the federal government; (2) the effects of the drug crisis on labor force participation and productivity and on people with disabilities and other vulnerable populations; (3) key federal efforts to reduce the availability of illicit drugs; and (4) agency efforts around drug education and prevention. We will determine whether this issue should be added to the High-Risk List once we have completed this ongoing and planned work.

## High-Risk Areas That Made Progress

Agencies can show progress by addressing our five criteria for removal from the list: leadership commitment, capacity, action plan, monitoring, and demonstrated progress.[9] As shown in table 1, 24 high-risk areas, or about two-thirds of all the areas, have met or partially met all five criteria for removal from our High-Risk List; 20 of these areas fully met at least one criterion. Compared with our last assessment, 7 high-risk areas showed progress in one or more of the five criteria without regressing in any of the criteria. Ten high-risk areas have neither met nor partially met one or more criteria. Two areas showed mixed progress by increasing in at least one criterion and also declining in at least one criterion. Three

[9]Additional detail on our high-risk criteria and ratings is in appendix I on page 69 of the report.

areas declined since 2017. These changes are indicated by the up and down arrows in table 1.

**Table 1: 2017 High-Risk Areas Rated Against Five Criteria for Removal from GAO's High-Risk List**

| | | Number of criteria | | |
|---|---|---|---|---|
| **High-risk area** | **Change since 2017** | **Met** | **Partially met** | **Not met** |
| Department of Defense (DOD) Supply Chain Management | ↑ | 5 | 0 | 0 |
| Mitigating Gaps in Weather Satellite Data | ↑ | 5 | 0 | 0 |
| DOD Support Infrastructure Management | ↑ | 2 | 3 | 0 |
| Medicare Program & Improper Payments[a] | ↑ | 2 | 3 | 0 |
| DOD Financial Management | ↑ | 1 | 3 | 1 |
| DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management | ↑ | 1 | 3 | 1 |
| DOD Business Systems Modernization | ↑ | 0 | 5 | 0 |
| DOD Approach to Business Transformation | ↑↓ | 1 | 4 | 0 |
| USPS Financial Viability | ↑↓ | 1 | 3 | 1 |
| NASA Acquisition Management | ↓ | 1 | 4 | 0 |
| Transforming the Environmental Protection Agency's (EPA) Processes for Assessing and Controlling Toxic Chemicals | ↓ | 0 | 5 | 0 |
| Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks | ↓ | 0 | 3 | 2 |
| Strengthening Department of Homeland Security Management Functions | ● | 3 | 2 | 0 |
| DOD Contract Management | ● | 1 | 4 | 0 |
| DOD Weapon Systems Acquisition | ● | 1 | 4 | 0 |
| Enforcement of Tax Laws | ● | 1 | 4 | 0 |
| Ensuring the Cybersecurity of the Nation | ● | 1 | 4 | 0 |
| Improving the Management of IT Acquisitions and Operations | ● | 1 | 4 | 0 |
| Managing Federal Real Property | ● | 1 | 4 | 0 |
| Protecting Public Health through Enhanced Oversight of Medical Products | ● | 1 | 4 | 0 |
| Strategic Human Capital Management | ● | 1 | 3 | 1 |
| Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests | ● | 0 | 5 | 0 |
| Improving and Modernizing Federal Disability Programs | ● | 0 | 5 | 0 |
| Management of Federal Oil and Gas Resources | ● | 0 | 5 | 0 |
| Modernizing the U.S. Financial Regulatory System | ● | 0 | 5 | 0 |
| National Flood Insurance Program | ● | 0 | 5 | 0 |
| Strengthening Medicaid Program Integrity | ● | 0 | 5 | 0 |
| Resolving the Federal Role in Housing Finance | ● | 0 | 4 | 1 |

| High-risk area | Change since 2017 | Number of criteria: Met | Partially met | Not met |
|---|---|---|---|---|
| Improving Federal Oversight of Food Safety | ● | 0 | 3 | 2 |
| Managing Risks and Improving VA Health Care | ● | 0 | 2 | 3 |
| 2020 Decennial Census[b] | | 1 | 4 | 0 |
| Government-wide Personnel Security Clearance Process[b] | | 1 | 3 | 1 |
| Improving Federal Management of Programs that Serve Tribes and Their Members[b] | | 0 | 5 | 0 |
| U.S. Government's Environmental Liability[b] | | 0 | 1 | 4 |
| Funding the Nation's Surface Transportation System[c] | | | | |
| Pension Benefit Guaranty Corporation Insurance Programs[c] | | | | |

(↑ indicates one or more areas progressed; ↓ indicates one or more areas declined since 2017; ↑ ↓ indicates mixed progress; ● indicates no change)

Source: GAO. | GAO-19-157SP

[a]Medicare Program & Improper Payments was only rated on the Improper Payments program; we did not rate other elements of the Medicare program because the area is subject to frequent legislative updates and the program is in a state of transition.

[b]Four areas are receiving ratings for the first time because they were newly added in 2017 and 2018.

[c]Two high-risk areas were not rated because addressing them primarily involves congressional action (Funding the Nation's Surface Transportation System and Pension Benefit Guaranty Corporation Insurance Programs).

Figure 1 shows that since our 2017 update, the most progress was made on the action plan criterion—four high-risk areas received higher ratings. We rated two areas lower on leadership commitment and two areas lower on monitoring.

**Figure 1: High-Risk Areas' Progress and Regress on High-Risk Criteria Since 2017**


Source: GAO analysis of criteria for removal from the High-Risk List status. I GAO-19-157SP

## Leadership Attention Needed to Meet High-Risk Criteria

Table 2 shows that 17 of the 34 high-risk areas we rated have met the leadership commitment criterion while two high-risk area ratings regressed on leadership commitment from met to partially met since our last report.

Leadership commitment is the critical element for initiating and sustaining progress, and leaders provide needed support and accountability for managing risks. Leadership commitment is needed to make progress on the other four high-risk criteria. Table 2 shows that only three high-risk areas met the criterion for capacity, six met the criterion for action plan, and two met the criterion for demonstrated progress. One high-risk area—U.S. Government's Environmental Liability—has partially met only

one criterion since we added the area to our list in 2017 and the rest are not met.

**Table 2: 2019 High-Risk Area Ratings on Five Criteria for Removal from GAO's High-Risk List**

| | Criteria | | | | |
|---|---|---|---|---|---|
| **High-risk area** | **Leadership commitment** | **Capacity** | **Action plan** | **Monitoring** | **Demonstrated progress** |
| Department Of Defense (DOD) Supply Chain Management | ★ | ★ | ★ | ★ | ★ |
| Mitigating Gaps in Weather Satellite Data | ★ | ★ | ★ | ★ | ★ |
| Strengthening Department of Homeland Security Management Functions | ★ | ☆ | ★ | ★ | ☆ |
| Medicare Program & Improper Payments[a] | ★ | ★ | ☆ | ☆ | ☆ |
| DOD Support Infrastructure Management | ★ | ☆ | ★ | ☆ | ☆ |
| 2020 Decennial Census | ★ | ☆ | ☆ | ☆ | ☆ |
| DOD Contract Management | ★ | ☆ | ☆ | ☆ | ☆ |
| DOD Weapon Systems Acquisition | ★ | ☆ | ☆ | ☆ | ☆ |
| Enforcement of Tax Laws | ★ | ☆ | ☆ | ☆ | ☆ |
| Ensuring the Cybersecurity of the Nation | ★ | ☆ | ☆ | ☆ | ☆ |
| Improving the Management of Information Technology Acquisitions and Operations | ★ | ☆ | ☆ | ☆ | ☆ |
| Managing Federal Real Property | ★ | ☆ | ☆ | ☆ | ☆ |
| Protecting Public Health through Enhanced Oversight of Medical Products | ★ | ☆ | ☆ | ☆ | ☆ |
| DOD Approach to Business Transformation | ☆ | ☆ | ★ | ☆ | ☆ |
| NASA Acquisition Management | ☆ | ☆ | ★ | ☆ | ☆ |
| DOD Financial Management | ★ | ☆ | ☆ | ☆ | ☆ |
| Strategic Human Capital Management | ★ | ☆ | ☆ | ☆ | ☆ |
| Government-wide Personnel Security Clearance Process | ★ | ☆ | ☆ | ☆ | ☆ |
| DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management | ★ | ☆ | ☆ | ☆ | ☆ |

| High-risk area | Criteria | | | | |
|---|---|---|---|---|---|
| | Leadership commitment | Capacity | Action plan | Monitoring | Demonstrated progress |
| USPS Financial Viability | ☆ | ☆ | ☆ | ★ | ☆ |
| DOD Business Systems Modernization | ☆ | ☆ | ☆ | ☆ | ☆ |
| Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests | ☆ | ☆ | ☆ | ☆ | ☆ |
| Improving and Modernizing Federal Disability Programs | ☆ | ☆ | ☆ | ☆ | ☆ |
| Improving Federal Management of Programs that Serve Tribes and Their Members | ☆ | ☆ | ☆ | ☆ | ☆ |
| Management of Federal Oil and Gas Resources | ☆ | ☆ | ☆ | ☆ | ☆ |
| Modernizing the U.S. Financial Regulatory System | ☆ | ☆ | ☆ | ☆ | ☆ |
| National Flood Insurance Program | ☆ | ☆ | ☆ | ☆ | ☆ |
| Strengthening Medicaid Program Integrity | ☆ | ☆ | ☆ | ☆ | ☆ |
| Transforming the Environmental Protection Agency's (EPA) Processes for Assessing and Controlling Toxic Chemicals | ☆ | ☆ | ☆ | ☆ | ☆ |
| Resolving the Federal Role in Housing Finance | ☆ | ☆ | ☆ | ☆ | ☆ |
| Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks | ☆ | ☆ | ☆ | ☆ | ☆ |
| Improving Federal Oversight of Food Safety | ☆ | ☆ | ☆ | ☆ | ☆ |
| Managing Risks and Improving VA Health Care | ☆ | ☆ | ☆ | ☆ | ☆ |
| U.S. Government's Environmental Liability | ☆ | ☆ | ☆ | ☆ | ☆ |

Legend: ★ Met ☆ Partially Met ☆ Not Met

Source: GAO. | GAO-19-157SP

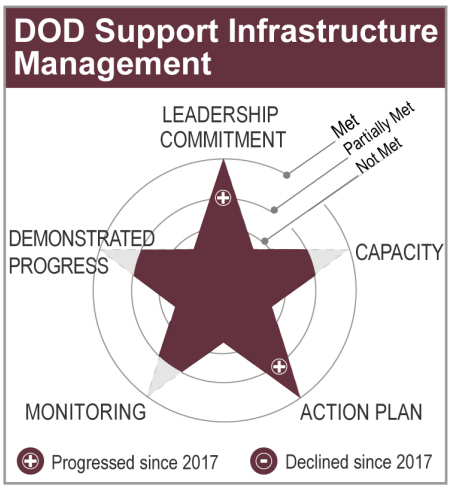
Notes: Two high-risk areas—Funding the Nation's Surface Transportation System and Pension Benefit Guaranty Corporation Insurance Programs—did not receive ratings against the five high-risk criteria because progress would primarily involve congressional action.

[a]Medicare Program & Improper Payments was only rated on the Improper Payments , and we did not rate other elements of the Medicare program

## Progress in High-Risk Areas

As noted, seven areas showed improvement in one or more criterion without regressing in any criteria. Two areas showed sufficient progress to be removed from the High-Risk List. The other five high-risk areas remaining on the 2019 list demonstrated improvement and are described below. Three of these five improving high-risk areas are the responsibility

of the Department of Defense (DOD)—DOD Support Infrastructure Management, DOD Financial Management, and DOD Business Systems Modernization. The two other improving areas are Department of Energy's (DOE's) Contract Management for the National Nuclear Security Administration and Office of Environmental Management, and Medicare Program & Improper Payments.




Source: GAO analysis. | GAO-19-157SP

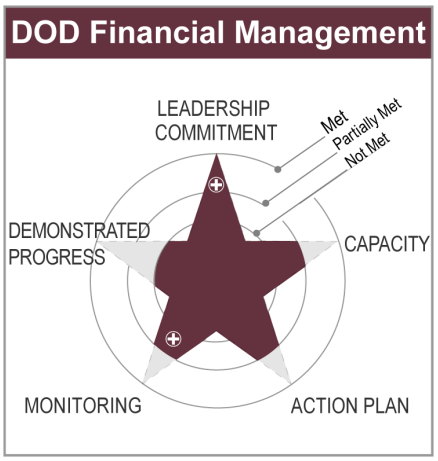
**DOD Support Infrastructure Management:** DOD manages a portfolio of real property assets that, as of fiscal year 2017, reportedly included about 586,000 facilities—including barracks, maintenance depots, commissaries, and office buildings. The combined replacement value of this portfolio is almost $1.2 trillion and includes about 27 million acres of land at nearly 4,800 sites worldwide. This infrastructure is critical to maintaining military readiness, and the cost to build and maintain it represents a significant financial commitment. Since our 2017 High-Risk Report, DOD's rating for two criteria—leadership commitment and action plan—improved from partially met to met.

DOD has demonstrated leadership commitment by stating its commitment to addressing key recommendations we have made by, for example, (1) better forecasting the initial Base Realignment and Closure (BRAC) costs for military construction, IT, and relocating military personnel and equipment; (2) better aligning infrastructure to DOD force structure needs by, for example, improving the accuracy and sufficiency of its excess capacity estimates; and (3) pursuing an effort to consolidate and standardize leases, which includes analyzing whether it is feasible to relocate functions from commercial leased space to existing space on an installation, thereby reducing leases and better utilizing excess space.

DOD has developed action plans to better identify excess infrastructure and thus be positioned to dispose of it. For example, in the 2017 High-Risk Report, we stated that DOD's Real Property Efficiency Plan includes DOD's goals for reducing the footprint of its real property inventory and metrics to gauge progress, to be implemented by the end of 2020. We also found in 2018 that DOD was achieving cost savings and cost avoidances as it had begun using intergovernmental support agreements between military installations and local governments to obtain installation services, such as waste removal, grounds maintenance, and stray animal control. As a result of these and other actions, DOD now meets the action plan criterion for this high-risk area.

As of December 2018, 23 recommendations related to this high-risk area remain open. DOD continues to partially meet the criteria for capacity, monitoring, and demonstrated progress.

See page 158 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.




Source: GAO analysis. | GAO-19-157SP

**DOD Financial Management:** Since our 2017 High-Risk Report, ratings for the DOD Financial Management high-risk area improved for the criteria of leadership commitment and monitoring. For the leadership commitment criterion, the high-risk area rating improved from partially met to met in 2019 due to several DOD leadership actions. For example, in 2018, DOD leadership met the goal of undergoing an agency-wide financial statement audit and established a process to remediate any audit findings—ultimately to improve the quality of financial information that is most valuable in managing the department's day-to-day operations. In addition, according to a DOD official, audit remediation efforts have produced benefits in certain inventory processes that have led to operational improvements.

DOD leadership demonstrated its commitment to making needed improvements by developing a database that tracks hundreds of findings and recommendations that came out of the audits. In addition, senior leadership has been meeting bimonthly with military services' leadership for updates on the status of corrective action plans to address audit findings and recommendations, and the Under Secretary of Defense (Comptroller) has been meeting frequently with the Secretary of Defense to review the plans.

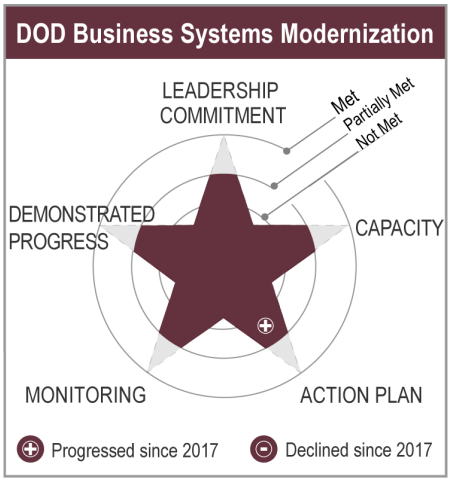
These same DOD actions also led to the high-risk area's rating for the criterion of monitoring to improve from not met to partially met. For example, the database mentioned above is intended to capture, prioritize, and assign responsibility for auditor findings and related corrective action plans, which are meant to be used to measure progress towards achieving a clean audit opinion.

Further, DOD leadership has held frequent meetings to discuss the status of corrective action plans. In addition, DOD also established councils in certain areas (e.g., financial reporting) to review the status of audit remediation activities and challenges. All of these actions demonstrate an improvement in DOD's monitoring activities for its financial management function.

However, DOD's efforts to improve its financial management continue to be impaired by long-standing issues—including its decentralized environment; cultural resistance to change; lack of skilled financial management staff; ineffective processes, systems, and controls; incomplete corrective action plans; and the need for more effective monitoring and reporting. DOD remains one of the few federal entities that cannot accurately account for and report on its spending or assets.

As of December 2018, 53 recommendations for this high-risk area are open. The DOD Financial Management high-risk area continues to partially meet the capacity and action plan criteria and not meet the demonstrated progress criterion.

See page 147 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.



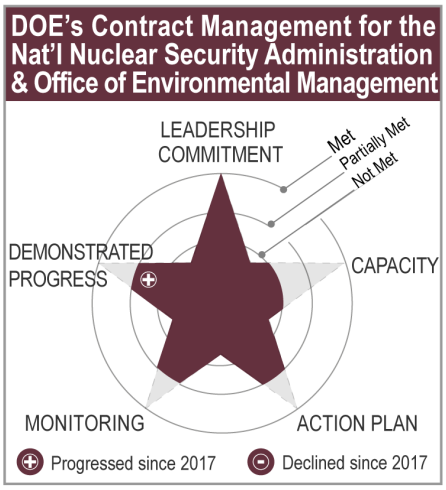

Source: GAO analysis. | GAO-19-157SP

**DOD Business Systems Modernization:** DOD spends billions of dollars each year to acquire modernized systems, including systems that address key areas such as personnel, financial management, health care, and logistics. This high-risk area includes three critical challenges facing DOD: (1) improving business system acquisition management, (2) improving business system investment management, and (3) leveraging DOD's federated business enterprise architecture.

DOD's capacity for modernizing its business systems has improved over time and, since our 2017 High-Risk Report, DOD's overall rating for the criterion of action plan improved from not met to partially met in 2019. DOD established a plan for improving its federated business enterprise architecture (i.e., description of DOD's current and future business environment and a plan for transitioning to the future environment). Specifically, the rating improved for DOD's federated business enterprise architecture segment of the high-risk area because DOD's assistant deputy chief management officer approved a business architecture improvement plan in January 2017.

Since 2017, we have made 10 recommendations related to this high-risk issue. As of December 2018, 27 recommendations are open. The leadership, capacity, monitoring, and demonstrated progress criteria remain partially met as in 2017.

See page 152 of the report for additional detail on this high-risk area, including more details on actions that need to be taken. .




Source: GAO analysis. | GAO-19-157SP

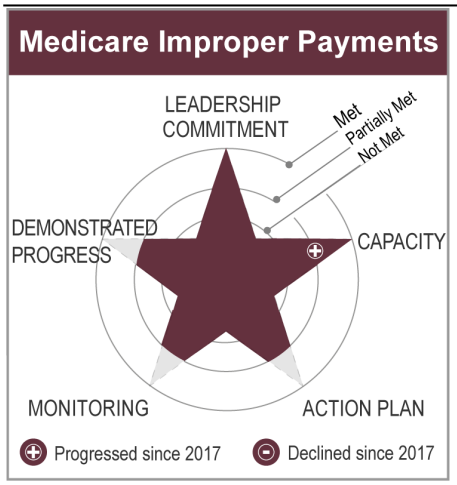
**DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management:** DOE oversees a broad range of programs related to nuclear security, science, energy, and waste cleanup, among other areas. As the largest civilian contracting agency in the federal government, DOE relies primarily on contractors to carry out its programs. For instance, DOE spends about 90 percent of its annual budget on contracts and acquiring capital assets. In fiscal year 2018, DOE's budget was $34.5 billion.

The high-risk area focuses on contracts, as well as major projects—those with an estimated cost of $750 million or greater—managed by DOE's National Nuclear Security Administration (NNSA) and Office of Environmental Management (EM).

Since our 2017 High-Risk Report, DOE has made progress by improving from a not met to a partially met rating for the demonstrated progress criterion. Specifically, through its Office of Cost Estimating and Program Evaluation, NNSA has enhanced its capability to estimate costs and schedules, and to assess alternatives for programs and projects, among other things. NNSA also made progress by adopting best practices in several areas, such as those for estimating costs and schedules in nuclear weapons refurbishment activities and capital asset acquisitions. For example, we determined that DOE's revised cost estimate of $17.2 billion to construct a Mixed Oxide Fuel Fabrication Facility to dispose of surplus, weapons-grade plutonium substantially met best practices—providing assurance that the estimated costs could be considered reliable. This finding contributed to DOE's reevaluation of the project and ultimate termination, in October 2018, in favor of a potentially less costly disposal approach.

Fifty-one of our recommendations were open as of December 2018; 15 recommendations were made since the last high-risk update in February 2017. DOE continues to meet the criterion of leadership commitment, partially meet the criteria for action plan and monitoring, and not meet the criterion for capacity.

See page 217 of the report for additional detail on this high-risk area, including more details on actions that need to be taken. .




Source: GAO analysis. | GAO-19-157SP

**Medicare Program & Improper Payments:** In calendar year 2017, Medicare, which is overseen by the Centers for Medicare & Medicaid Services (CMS), financed $702 billion worth of health services for approximately 58 million elderly and disabled beneficiaries. Medicare faces a significant risk with improper payments—payments that either were made in an incorrect amount or should not have been made at all—which reached an estimated $48 billion in fiscal year 2018.

Since our 2017 High-Risk Report, estimated improper payment rates declined more than one percent across the Medicare program. In addition, CMS' rating for the capacity criterion of the improper payments segment improved from partially met to met in 2019 due to several actions. First, the Center for Program Integrity's (CPI) budget and resources have increased over time and the agency has established work groups and interagency collaborations to extend its capacity. For example, CMS allocated more staff to CPI after Congress provided additional funding. CPI's full-time equivalent positions increased from 177 in 2011 to 419 in 2017.

Additionally, in August 2017, we reported that CMS's Fraud Prevention System, which analyzes claims to identify health care providers with suspect billing patterns, helped speed up certain fraud investigation processes. Further, the Healthcare Fraud Prevention Partnership helped improve information sharing among payers inside and outside of the government.

Since 1990, when we added Medicare to our High-Risk List, we have made many recommendations related to the Medicare program, 28 of which were made since the last high-risk update in February 2017. As of December 2018, more than 80 recommendations remain open. CMS continues to meet the criterion of leadership commitment and to partially meet the remaining three criteria of action plan, monitoring, and demonstrated progress.

See page 241 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Congressional Action Aided Progress on High-Risk Issues

Congress enacted several laws since our last report in February 2017 to help make progress on high-risk issues. Table 3 lists selected examples of congressional actions taken on high-risk areas.

**Table 3: Examples of Congressional Actions Taken on High-Risk Areas**

| High-risk area | Congressional actions taken | How GAO work contributed to congressional actions | Impact on high-risk area |
|---|---|---|---|
| **Department of Defense (DOD) Approach to Business Transformation** | Section 901(c) of the National Defense Authorization Act (NDAA) for Fiscal Year 2017 created the position of Chief Management Officer (CMO) within DOD, effective February 1, 2018.[a] | The 2016 passage of the NDAA is consistent with our February 2005 report, in which we identified the need for DOD to have a full-time CMO position created through legislation, with responsibility, authority, and accountability for DOD's overall business transformation efforts. | Based on congressional direction, DOD established and is beginning to restructure its CMO office to fulfill its responsibilities given by Congress. Continued leadership commitment at the highest levels will help sustain focus on this business transformation. The longer this critical position is filled by someone in an acting capacity, the greater the risk that DOD's transformation efforts could be impacted. (**Leadership commitment**) |
| **Improving the Management of Information Technology (IT) Acquisitions and Operations** | Subtitle G of title X of the NDAA for Fiscal Year 2018 established a Technology Modernization Fund and Board, and allowed agencies to establish agency information technology system modernization and working capital funds.[b] | We identified the need to better manage the billions of dollars the federal government spends annually on legacy IT when we added this area to the High-Risk List in 2015. We further examined the government's heavy reliance on legacy IT systems in our 2016 report. | These provisions (1) allowed agencies to establish working capital funds for use in transitioning away from legacy IT systems and (2) created a technology modernization fund to help agencies retire and replace legacy systems, as well as acquire or develop new systems. (**Capacity**) |
| **Government-wide Personnel Security Clearance Process** | Section 925(k) of the NDAA for Fiscal Year 2018 requires the Director of National Intelligence, in coordination with the Chair and other principals of the Suitability, Security, and Credentialing Performance Accountability Council, to provide an annual assessment of any impediments to the timely processing of personnel security clearances.[c] | The 2017 passage of the NDAA is consistent with our December 2017 report, in which we asked Congress to consider both reinstating and adding to the requirement in the Intelligence Reform and Terrorism Prevention Act of 2004 for the executive branch to report to appropriate congressional committees annually on its background investigation process. | Annual assessments will help Congress monitor the timeliness of the executive branch's background investigations to monitor its own timeliness. The act requires the executive branch to report the length of time for initiating and conducting investigations and finalizing adjudications, and case load composition and costs, among other matters deemed relevant by Congress. (**Monitoring**) |

| High-risk area | Congressional actions taken | How GAO work contributed to congressional actions | Impact on high-risk area |
|---|---|---|---|
| **Mitigating Gaps in Weather Satellite Data** | Provisions of the NDAA for Fiscal Year 2015 limited the availability of certain funds until the Secretary of Defense submitted to congressional defense committees a plan related to weather satellites.[d] Similarly, the NDAA for Fiscal Year 2016 limited the availability of certain funds until (1) the Secretary of Defense briefed the congressional defense committees on a plan for cloud characterization and theater weather imagery, and (2) the Chairman of the Joint Chiefs of Staff certified to the committees that the plan would meet DOD requirements without negatively affecting commanders of combatant commands.[e] | We found that DOD was slow to establish plans for its Weather System Follow-on–Microwave program in our 2017 High-Risk Report. We also found it had made little progress in determining how it would meet weather satellite requirements for cloud descriptions and area-specific weather imagery. | These provisions (1) encouraged DOD to develop and implement plans to address its weather satellite requirements and (2) helped Congress monitor DOD plans and actions to address these requirements. (**Action plan**) |
| **Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks** | Section 1234(a)(5) of the Disaster Recovery Reform Act of 2018 allows the President to set aside, with respect to each major disaster, a percentage of certain grants to use for pre-disaster hazard mitigation. Section 1206(a)(3) makes federal assistance available to state and local governments for building code administration and enforcement.[f] | We found that federal investments in resilience could be more effective if post-disaster hazard mitigation efforts were balanced with resources for pre-disaster hazard mitigation, as part of a comprehensive resilience investment strategy. We also found that enhancing state and local disaster resilience could help reduce federal fiscal exposure. | These provisions could improve state and local resilience to disasters by increasing the amount of funding available for pre-disaster hazard mitigation and increasing state and local adoption and enforcement of the latest building codes. (**Capacity**) |
| **Ensuring the Cybersecurity of the Nation** | An explanatory statement accompanying the Consolidated Appropriations Act, 2018 directed the National Protection and Programs Directorate to brief the appropriations committees on its specific plans to address GAO recommendations including the National Cybersecurity and Communications Integration Center's (NCCIC) implementation of the recommendations for ensuring that it fulfills its statutory functions, such as sharing information about cyber threats, by timely reporting information that is relevant and actionable, and establishing appropriate performance metrics.[g] | We reported that NCCIC had taken steps to perform each of the Department of Homeland Security's (DHS) statutorily required cybersecurity functions. However, the extent to which NCCIC performed the actions was unclear, in part, because the center had not yet established metrics and methods by which to evaluate its performance. | As of January 2019, DHS had fully addressed two of the nine recommendations we made to enhance the effectiveness and efficiency of NCCIC, and had taken initial actions toward addressing several others. (**Demonstrated progress**) |

| High-risk area | Congressional actions taken | How GAO work contributed to congressional actions | Impact on high-risk area |
|---|---|---|---|
| **Managing Risks and Improving VA Health Care** | The No Veterans Crisis Line Call Should Go Unanswered Act directs the Department of Veterans Affairs (VA) to develop a quality assurance document for carrying out the toll-free Veterans Crisis Line, and requires VA to develop a plan to ensure that each telephone call, text message, and other communication received is answered in a timely manner.[h] | About 6 months prior to the passage of this legislation, our May 2016 report identified the need for VA to take several steps to better test, track, and assess the performance of the Veterans Crisis Line in order to improve the timeliness and quality of its responses to veterans and others. | In July 2017, VA updated a quality assurance plan with measurable targets and time frames for key performance indicators needed to assess Veterans Crisis Line performance. VA also established an Executive Leadership Council in March 2017 to monitor data on the key performance indicators. These two actions will assist with the oversight and accountability of the Veterans Crisis Line, and the services provided to veterans. (**Leadership commitment, Action plan, and Monitoring**) |
| **Improving Federal Management of Programs that Serve Tribes and Their Members** | An explanatory statement accompanying the Consolidated Appropriations Act, 2018 directed the Indian Health Service (IHS) to report to the appropriations committees on the status of its efforts on improving wait times for patients seeking primary and urgent care, including an explanation of how these efforts will address GAO recommendations.[i] | We found that IHS had not conducted any systematic, agency-wide oversight of the timeliness of primary care in its federally operated facilities and recommended that IHS communicate specific agency-wide standards for patient wait times; monitor patient wait times; and ensure corrective actions are taken when standards are not met. | IHS developed specific standards for patient wait times and developed a plan and timeline for implementing an agency-wide standard for patient wait times. It is also in the process of updating its patient wait time policy to include emergency department wait times and developing automated data collection for wait times. (**Leadership commitment, Action plan, Monitoring**) |

Source: GAO analysis. | GAO-19-157SP

[a]Pub. L. No. 114-328, § 901(c), 130 Stat. 2000, 2341 (2016).

[b]Pub. L. No. 115-91, §§ 1076–1078, 131 Stat. 1283, 1586–1594 (2017).

[c]Pub. L. No. 115-91, § 925(k)(1)(F), (3)(I), 131 Stat. 1283, 1530, 1532 (2017).

[d]Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 1612, 128 Stat. 3292, 3628 (2014).

[e]National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 1615, 129 Stat. 726, 1105 (2015).

[f]FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. D, §§ 1206(a)(3), 1234(a)(5) 132 Stat. 3186, 3440, 3462 (2018).

[g]Chairman Rodney P. Frelinghuysen of the Committee on Appropriations of the House of Representatives filed an explanatory statement relating to the House amendment of H.R. 1625 in the Congressional Record on March 22, 2016. 164 Cong. Rec. H2045, H2557. Section 4 of the Consolidated Appropriations Act, 2018, states that this explanatory statement shall have the same effect with respect to the allocation of funds and implementation of divisions A through L of the act as if it were a joint explanatory statement of a committee of conference. Pub. L. No. 115-141, § 4, 132 Stat. 348, 350 (2018).

[h]Pub. L. No. 114-247, 130 Stat. 996 (2016).

[i]Chairman Rodney P. Frelinghuysen of the Committee on Appropriations of the House of Representatives filed an explanatory statement relating to the House amendment of H.R. 1625 in the Congressional Record on March 22, 2016. 164 Cong. Rec. H2045, H2628. Section 4 of the Consolidated Appropriations Act, 2018, states that this explanatory statement shall have the same effect with respect to the allocation of funds and implementation of divisions A through L of the act as if it were a joint explanatory statement of a committee of conference. Pub. L. No. 115-141, § 4, 132 Stat. 348, 350 (2018).

Congressional oversight also plays a vital role in addressing high-risk issues. For example, at a May 2018 hearing, we testified that the Census Bureau's (Bureau) cost estimate was not reliable, and that the actual cost could be higher than planned.[10] Further, the Secretary of Commerce created a dedicated team to provide oversight and guidance to the Bureau on cost estimation.

In addition to its instrumental role in supporting progress in individual high-risk areas, Congress also enacted the following statutes that, if implemented effectively, will help foster progress on high-risk issues government-wide:

- **Fraud Reduction and Data Analytics Act of 2015 (FRDAA):**[11] FRDAA is intended to strengthen federal antifraud controls. FRDAA requires OMB to use our Fraud Risk Framework[12] to create guidelines for federal agencies to identify and assess fraud risks, and then design and implement control activities to prevent, detect, and respond to fraud. Agencies, as part of their annual financial reports beginning in fiscal year 2017, are further required to report on their fraud risks and their implementation of fraud reduction strategies, which should help Congress monitor agencies' progress in addressing and reducing fraud risks.

  To aid federal agencies in better analyzing fraud risks, FRDAA requires OMB to establish a working group tasked with developing a plan for creating an interagency library of data analytics and data sets to facilitate the detection of fraud and the recovery of improper payments. This working group and the library should help agencies coordinate their fraud detection efforts and improve their ability to use data analytics to monitor databases for potential

[10]GAO, *2020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration,* GAO-18-543T (May 8, 2018).

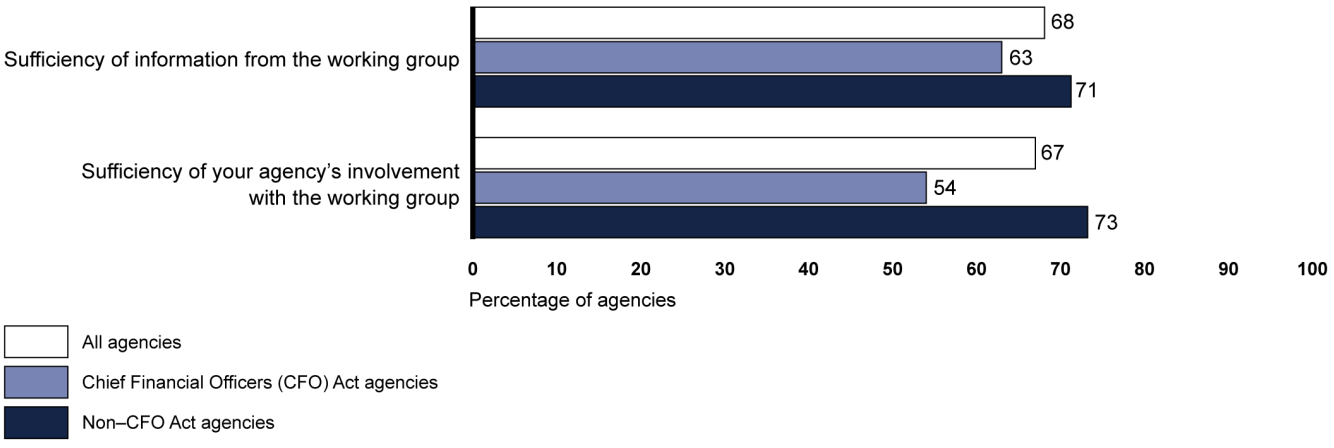
[11]Pub. L. No. 114-186, 130 Stat. 546 (2016).

[12]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

improper payments. The billions of dollars in improper payments, some of which may be a result of fraud, are a central part of the Medicare Program, Medicaid Program, and Enforcement of Tax Laws (Earned Income Tax Credit) high-risk areas.

We reported in 2018 that, among other things, OMB did not involve all agencies subject to the act as required by FRDAA or hold the required minimum number of working-group meetings in 2017.[13] As shown in figure 2, a majority of the 72 agencies surveyed indicated a lack of involvement with and information from the working group as challenges in implementing FRDAA. We made three recommendations, including that OMB ensure the working group meets FRDAA's requirements to involve all agencies that are subject to the act and ensure that mechanisms to share controls, best practices, and data-analytics techniques are in place. OMB did not concur with our recommendations. We continue to believe the recommendations are valid, as discussed in the 2018 report.

**Figure 2: Percentage of Agencies That Identified Their Involvement with the Fraud Reduction and Data Analytics Act of 2015 Working Group as a Great or Moderate Challenge**




Source: GAO analysis of survey data. | GAO-19-157SP

[13]GAO, *Fraud Risk Management: OMB Should Improve Guidelines and Working-Group Efforts to Support Agencies' Implementation of the Fraud Reduction and Data Analytics Act*, GAO-19-34 (Washington, D.C.: December 4, 2018).

- **IT Acquisition Reform, statutory provisions known as the Federal Information Technology Acquisition Reform Act (FITARA):**[14] FITARA, enacted in December 2014, was intended to improve how agencies acquire IT and better enable Congress to monitor agencies' progress in reducing duplication and achieving cost savings. Since the enactment of these provisions, OMB and federal agencies have paid greater attention to IT acquisition and operation, resulting in improvements to the government-wide management of this significant annual investment. These efforts have been motivated in part by sustained congressional support for improving implementation of this law, as highlighted in agencies' FITARA implementation scores issued biannually by the House Committee on Oversight and Reform.

  This continuing oversight has produced positive results. For example, in the committee's December 2018 FITARA implementation scorecard, 18 of the 24 major federal agencies received the highest possible rating for their efforts to improve the management of software licenses, of which we have found there are thousands annually across the government. Seven months earlier, in the prior scorecard, only eight agencies had achieved this rating. Moreover, federal agencies have taken actions to address 106 of the 136 related recommendations that we have made in this area since 2014.

  FITARA includes specific requirements related to seven areas: the federal data center consolidation initiative, enhanced transparency and improved risk management, agency Chief Information Officer authority enhancements, portfolio review, expansion of training and use of IT acquisition cadres, government-wide software purchasing, and maximizing the benefit of the federal strategic sourcing initiative.

  In November 2017, Congress extended or removed the sunset dates of several of these statutory requirements that were originally to end in 2018 and 2019.[15] While all of the 24 federal agencies covered by this law have developed FITARA implementation plans, the agencies need to effectively execute these plans. Successfully addressing FITARA requirements is

[14]FITARA was enacted into law as part of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (2014), div. A, title VIII, subtitle D, §§ 831-837, 128 Stat. 3292, 3438-3450.

[15]FITARA Enhancement Act of 2017, Pub. L. No. 115-88, 131 Stat. 1278 (2017).

central to making progress in Improving the Management of IT Acquisitions and Operations, which has been on our High-Risk List since 2015.

- **Program Management Improvement Accountability Act (PMIAA):**[16] Enacted in December 2016, the act is intended to improve program and project management in certain larger federal agencies. Among other things, the act requires the Deputy Director for Management of OMB to adopt and oversee implementation of government-wide standards, policies, and guidelines for program and project management in executive agencies. The act also requires the Deputy Director to conduct portfolio reviews to address programs we identify as high-risk. It further creates a Program Management Policy Council to act as the principal interagency forum for improving practices related to program and project management. The council is to review programs identified as high-risk and make recommendations to the Deputy Director or designee.

  OMB has produced a general strategy for implementing the law through 2022 and met some initial milestones required by PMIAA. For example, in June 2018, OMB issued OMB Memorandum M-18-19, which includes: (1) agency guidance for implementing PMIAA, (2) a five-year strategic outline for improving program and project management, and (3) initial program management standards and principles.[17] Further, agencies have designated Program Management Improvement Officers to guide their implementation of PMIAA.

  According to OMB, it began implementing PMIAA's requirement to conduct portfolio reviews on high-risk areas by requiring relevant agencies to provide several items for discussion during the 2018 Strategic Review meetings. These annual meetings are to consist primarily of a discussion of agency progress towards each of the strategic objectives outlined in their strategic plans, but also cover other management topics such as enterprise risk management and high-risk area progress. According to OMB documents, in advance of these meetings, OMB required agencies to provide a high-level summary of (1) any disagreements with our

[16]Pub. L. No. 114-264, 130 Stat. 1371 (2016).

[17]Office of Management and Budget, *Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA)*, OMB Memorandum M-18-19 (Washington, D.C.: June 25, 2018).

recommendations, (2) progress barriers, and (3) actions needed by OMB, other agencies, or Congress to help the agency achieve progress towards removal from our High-Risk List.

OMB officials told us their 2018 Strategic Review meetings did not address each high-risk area but did address government-wide high-risk areas, such as cybersecurity, information technology, and strategic human capital as they related to the President's Management Agenda.

In the past, senior management officials from OMB, applicable agencies, and our agency have met to address areas where additional management attention could be beneficial to high-risk issues. These trilateral meetings, beginning in 2007 and pre-dating PMIAA's 2016 enactment, have continued across administrations.

However, OMB has organized only one of these high-risk meetings since the last high-risk update in 2017, on the Government-wide Personnel Security Clearance Process. In November 2018, OMB told us of plans to hold additional meetings on priority high-risk areas, including the 2020 Decennial Census, Strategic Human Capital Management, Ensuring the Cybersecurity of the Nation, National Aeronautics and Space Administration (NASA) Acquisition Management, and Managing Federal Real Property.

Effective implementation of PMIAA provides an important opportunity to enhance progress on high-risk areas by focusing leadership attention through the portfolio reviews and trilateral meetings. Further, a number of high-risk areas have longstanding or significant program and project management concerns, including the acquisition-related high-risk areas for DOD, DOE, NASA, and VA. These and other programs can benefit from improving program and project management. In December 2019, we will report on OMB's progress in implementing PMIAA, including what further steps it has taken to use the portfolio review process required in PMIAA to address issues on our High-Risk List.

## Executive Branch Action on Our Recommendations Aided Progress on High-Risk Issues

Agency leaders took actions to implement our recommendations. These resulted in numerous improvements to programs and operation and improved service. Further, these actions to implement our recommendations resulted in significant financial benefits. Table 4 shows

some examples of the financial benefits achieved since our last High-Risk Report.

**Table 4: Examples of GAO High-Risk Area Recommendations Leading to Financial Benefits**

| High-risk area | GAO recommendations leading to financial benefits | Financial benefits achieved |
|---|---|---|
| **Strengthening Medicaid Program Integrity** | In multiple reports, we found that demonstration spending limits approved by the Department of Health and Human Services (HHS) often were not budget neutral, as required by HHS policy. This increased the federal government's fiscal liability by billions of dollars. We recommended that HHS better ensure that valid methods are used to determine spending limits. | HHS responded by limiting the amount of unspent funds states may accrue and reducing the federal government's fiscal liability. As a result, the Centers for Medicare & Medicaid Services was able to identify a total of $23.5 billion in financial benefits for fiscal year (FY) 2017. |
| **Improving the Management of Information Technology (IT) Acquisitions and Operations** | In multiple reports, we made recommendations for improving the management of IT portfolios, which resulted in reduced agency commodity IT spending and fewer duplicative investments. | Agencies have achieved about $2.5 billion in savings from fiscal years 2012 to 2017 through the Office of Management and Budget's PortfolioStat that was intended to consolidate and eliminate duplicative systems. Agencies have the potential to achieve about $3.5 billion in additional savings. |
| **Resolving the Federal Role in Housing Finance** | In June 2013, we recommended actions for the Federal Housing Administration (FHA) to increase returns on sales of foreclosed properties with FHA-insured mortgages. | FHA's actions in response to our recommendations improved its returns and led to financial benefits totaling about $1.3 billion in 2017. |
| **Medicare Program & Improper Payments** | In December 2015, we recommended that Congress consider directing the Secretary of HHS to equalize payment rates between physician offices and hospital outpatient departments for evaluation and management services and to return the associated savings to the Medicare program. | This change in reimbursement resulted in estimated cost savings to the program of $1.6 billion in FYs 2017 and 2018, and will result in additional savings going forward. |
| **Enforcement of Tax Laws** | In June 2015, we expressed concerns to Internal Revenue Service (IRS) officials about fraudsters potentially using taxpayer account information stolen in the 2014 and 2015 "Get Transcript" online service data breach to file multiple fraudulent returns and receive refunds. In response, IRS changed its authentication and monitoring procedures for accounts affected by the breach. | As a result of our suggestion and the new authentication procedures, in August 2017 we found that IRS prevented paying a total of $480.2 million in fraudulent refunds in FYs 2015 and 2016. In 2018, we found that IRS prevented an additional $110 million in FY 2017. |
| **National Flood Insurance Program** | Staff from the Federal Emergency Management Administration (FEMA) identified a number of actions that the agency has taken or has underway to address issues we raised related to its rate-setting methods in June 2011. In response to a congressional matter we made, congressional staff notified us that Congress passed the Biggert-Waters Flood Insurance Reform Act of 2012 which eliminated or phased out subsidized premium rates for several types of properties. | As a result of changes FEMA has made in rates for certain subsidized properties, we estimate that policyholders with these subsidized premiums paid $338.4 million (net present value) more in premiums as of the end of FY 2017 than they would have paid prior to the enactment of the Biggert-Waters Act. |

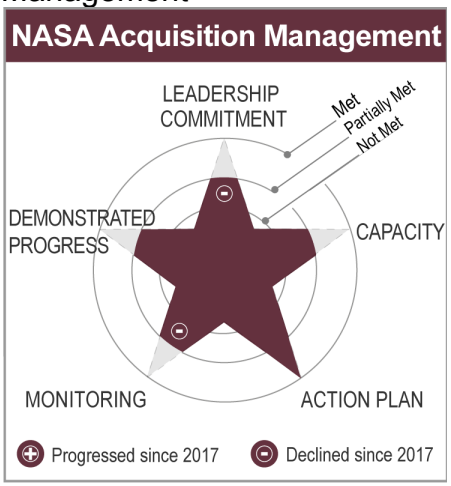
Source: GAO analysis. | GAO-19-157SP

# High-Risk Areas Needing Significant Attention

In the 2 years since our last High-Risk Report, three areas—NASA Acquisition Management, Transforming EPA's Process for Assessing and Controlling Toxic Chemicals, and Limiting the Federal Government's Fiscal Exposure By Better Managing Climate Change Risks—have regressed in their ratings against our criteria for removal from the High-Risk List. In addition, while progress is needed across all high-risk areas, we have identified nine additional areas that require significant attention to address imminent, longstanding, or particularly broad issues affecting the nation.

## Three High-Risk Areas That Regressed

### NASA Acquisition Management




Source: GAO analysis. | GAO-19-157SP

NASA plans to invest billions of dollars in the coming years to explore space, improve its understanding of the Earth's environment, and conduct aeronautics research, among other things. We designated NASA's acquisition management as high risk in 1990 in view of NASA's history of persistent cost growth and schedule delays in the majority of its major projects.

Following several years of continuing a generally positive trend of limiting cost growth and schedule delays for its portfolio of major projects, we found that NASA's average launch delay increased from 7 to 12 months between May 2017 and May 2018. Further, the overall development cost growth increased from 15.6 percent to at least 18.8 percent over the same time period. NASA's largest science project, the James Webb Space Telescope, has experienced schedule delays of 81 months and cost growth of 95 percent since the project's cost and schedule baseline was first established in 2009.

NASA is at risk for continued cost growth and schedule delays in its portfolio of major projects. Since our 2017 high-risk update, we have lowered NASA acquisition management from meeting the rating to partially meeting the rating in two criteria—leadership commitment and monitoring. The other three criteria ratings remained the same as in 2017. Ratings for capacity and demonstrated progress remain partially met and the rating for action plan remains met.

Over the next several years, NASA plans to add new, large, and complex projects to the portfolio, including a lunar Gateway—currently being discussed as a platform in a lunar orbit to mature deep space exploration capabilities. In addition, many of NASA's current major projects, including

some of the most expensive ones, are in the phase of their life cycles when cost growth and schedule delays are most likely.

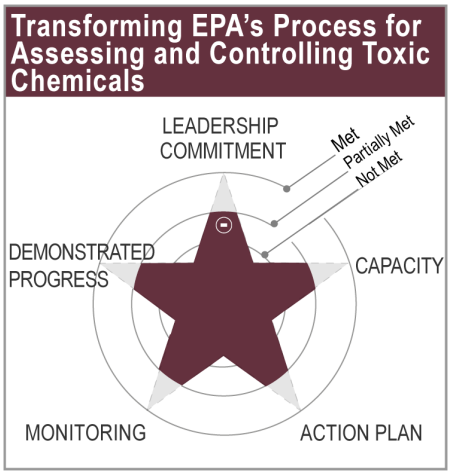
NASA acquisition management requires significant attention for the following reasons:

- NASA leadership has approved risky programmatic decisions for complex major projects, which compounded technical challenges. For example, leadership has approved some programs to proceed (1) with low cost and schedule reserves, (2) with overly aggressive schedules, and (3) without following best practices for establishing reliable cost and schedule baselines.
- NASA leadership has also not been transparent about cost and schedule estimates for some of its most expensive projects. Without transparency into these estimates, both NASA and Congress have limited data to inform decision making.
- NASA has not yet instituted a program for monitoring and independently validating the effectiveness and sustainability of the corrective action measures in its new action plan, which NASA finalized in December 2018.

In addition, while NASA has taken some steps to build capacity to help reduce acquisition risk, including updating tools aimed at improving cost and schedule estimates, other areas still require attention. For example, we reported in May 2018 that several major NASA projects experienced workforce challenges, including not having enough staff or staff with the right skills. NASA has also identified capability gaps in areas such as scheduling, earned value management, and cost estimating, and has efforts underway to try to improve capacity in these areas.

Since 2017, we have made 9 recommendations on this high-risk area, and as of December 2018, 15 recommendations remain open. These recommendations include that NASA needs to improve transparency of major project cost and schedule estimates, especially for its human spaceflight programs, as well as continue to build capacity to reduce acquisition risk. NASA will also need to implement its new action plan and track progress against it. See page 222 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Transforming EPA's Process for Assessing and Controlling Toxic Chemicals




Source: GAO analysis. | GAO-19-157SP

The Environmental Protection Agency's (EPA's) ability to effectively implement its mission of protecting public health and the environment is dependent on it assessing the risks posed by chemicals in a credible and timely manner. Such assessments are the cornerstone of scientifically sound environmental decisions, policies, and regulations under a variety of statutes.

Based on our work since our 2017 High-Risk Report, the overall rating for leadership commitment decreased from met to partially met due to limited information for completing chemical assessments and proposed budget cuts in the Integrated Risk Information System (IRIS) Program. The ratings for the remaining four criteria remain unchanged and are partially met.

The EPA Acting Administrator indicated his commitment to fulfill the agency's obligations under the Toxic Substances Control Act (TSCA) as amended by the 2016 Frank R. Lautenberg Chemical Safety for the 21 Century Act (Lautenberg Act) and ensure chemicals in the marketplace are safe for human health and the environment. Nonetheless, EPA needs to give more attention to several areas to fully realize the benefits of the new law, and to demonstrate additional progress in the IRIS Program, such as:

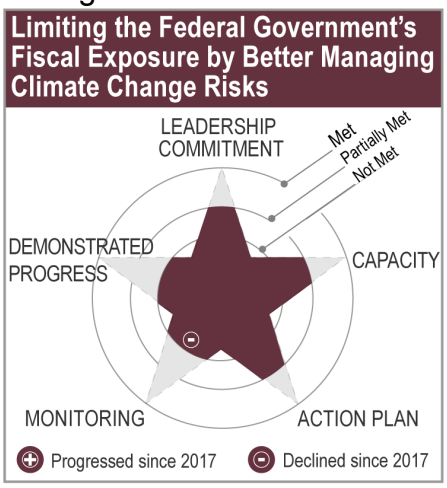
- While EPA released a document in late December 2018 called the IRIS Program Outlook, the Outlook fails to list the projected date for most of the assessments and includes no information regarding assessment prioritization—including how these assessments will meet program and regional office needs.
- The Lautenberg Act increases both EPA's responsibility for regulating chemicals and its workload. EPA recently issued a rule under the act to collect fees from certain companies to defray a portion of the implementation costs, but it is unclear whether the fees collected will be sufficient to support relevant parts of the program.
- EPA issued a First Year Implementation Plan in June 2016 noting that this document is intended to be a roadmap of major activities EPA will focus on during the initial year of implementation. As of mid-February 2019 the plan has not been updated, according to publically available information, although EPA had indicated that it is a living document that will be further developed over time.

EPA needs to ensure that the people and resources dedicated to the IRIS Program and TSCA implementation are sufficient. Our March 2019 report on chemical assessments provides information on what remains to

be done to address challenges in the IRIS program and implement the Lautenberg Act.[18]

Since we added this area to our High-Risk List in 2009, we have made 12 recommendations to EPA related to IRIS and TSCA. As of February 2019, seven recommendations remain open. See page 204 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks




Source: GAO analysis. | GAO-19-157SP

Numerous studies have concluded that climate change poses risks to many environmental and economic systems and creates a significant fiscal risk to the federal government. The rising number of natural disasters and increasing reliance on the federal government for assistance is a key source of federal fiscal exposure. As of December 2018, total federal funding for disaster assistance since 2005 is approaching half a trillion dollars (about $430 billion), most recently for catastrophic hurricanes, flooding, wildfires, and other losses in 2017 and 2018. The costliness of disasters is projected to increase as extreme weather events become more frequent and intense due to climate change. There are five areas where government-wide action is needed to reduce federal fiscal exposure, including, but not limited to, the federal government's role as (1) the insurer of property and crops; (2) the provider of disaster aid; (3) the owner or operator of infrastructure; (4) the leader of a strategic plan that coordinates federal efforts and informs state, local, and private-sector action; and (5) the provider of data and technical assistance to decision makers.

Neither global efforts to mitigate climate change causes nor regional adaptation efforts currently approach the scales needed to avoid substantial damages to the U.S. economy, environment, and human health over the coming decades, according to the November 2018 Fourth National Climate Assessment. Government-wide action is needed to improve the nation's resilience to natural hazards and reduce federal fiscal exposure to climate change impacts.

Congress continues to show its commitment to progress on this high-risk issue by enacting legislation. For example, in October 2018, the Disaster Recovery Reform Act was enacted, which, among other things, allows the President to set aside, with respect to each major disaster, a percentage

[18]GAO, *Chemical Assessments: Status of EPA's Efforts to Produce Assessments and Implement the Toxic Substances Control Act.* GAO-19-270. Washington, D.C.: March 4, 2019.

of certain grants to use for pre-disaster hazard mitigation. In addition, the National Defense Authorization Act of 2018, required, among other things, DOD to report on climate impacts to its installations. However, the federal government has not made measurable progress since 2017 to reduce its fiscal exposure to climate change, and in some cases, has revoked prior policies designed to do so. Specifically, since 2017, the ratings for four criteria remain unchanged—three at partially met and one at not met. The rating for one criterion—monitoring—regressed to not met.

Limiting the federal government's fiscal exposure to climate change requires significant attention because the federal government has revoked prior policies that had partially addressed this high-risk area and has not implemented several of our recommendations that could help reduce federal fiscal exposure. For example, since our 2017 high-risk update, the federal government:

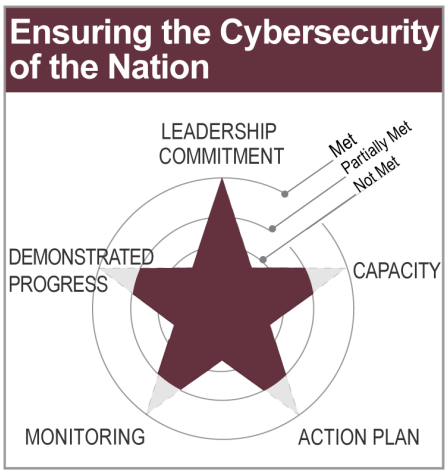
- revoked Executive Order 13690, which had established a government-wide federal flood risk management standard to improve the resilience of communities and federal assets against the impacts of flooding. This action could increase federal fiscal exposure, as taxpayer-funded projects may not last as long as intended because they are not required to account for future changes in climate-related risk.
- rescinded its guidance directing agencies to consider climate change in their National Environmental Policy Act of 1969 reviews for certain types of federal projects.
- has not implemented our July 2015 recommendation to establish a comprehensive investment strategy identifying, prioritizing, and implementing federal disaster resilience investments that could reduce federal fiscal exposure to climate change.
- has not implemented our November 2015 recommendations to create a national climate information system providing authoritative, accessible information useful for state, local, and private-sector decision making.

We have made 62 recommendations related to this high-risk area, 12 of which were made since our February 2017 high-risk update. As of December 2018, 25 remain open. The federal government needs a cohesive strategic approach with strong leadership and the authority to manage climate change risks across the entire range of federal activities.

See page 110 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Additional High-Risk Areas That Need Significant Attention

### Ensuring the Cybersecurity of the Nation




Source: GAO analysis. | GAO-19-157SP

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being. The risks to systems underpinning the nation's critical infrastructure are increasing as security threats evolve and become more sophisticated.

We first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. In 2018, we updated this high-risk area to reflect the lack of a comprehensive cybersecurity strategy for the federal government.

Since 2010, we have made over 3,000 recommendations to agencies aimed at addressing cybersecurity shortcomings, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Of those 3,000 recommendations, 448 were made since our last high-risk update in February 2017. Although many recommendations have been addressed, about 700 have not yet been implemented.

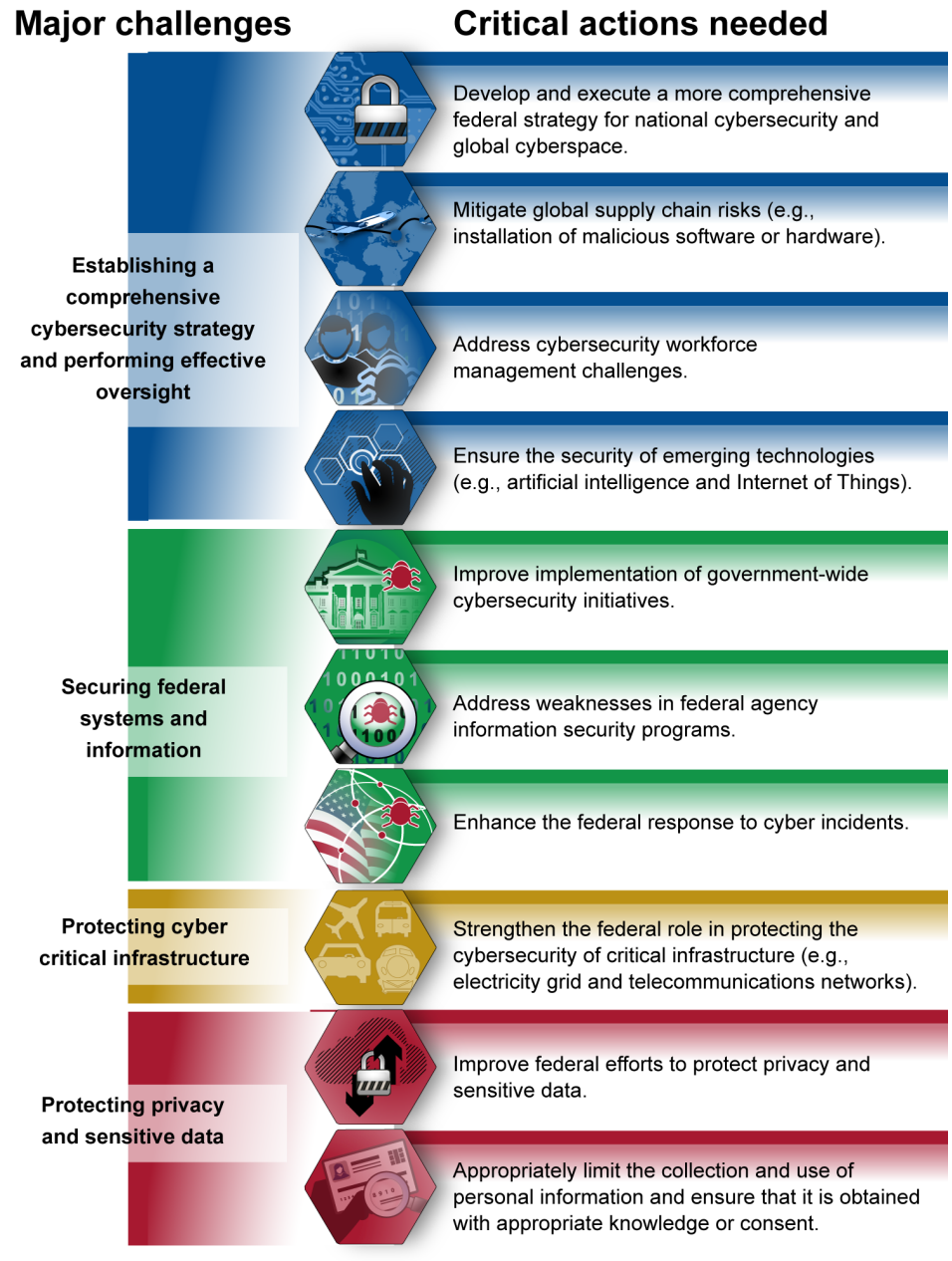
Despite the number of unimplemented recommendations, since our 2017 High-Risk Report, the administration has made progress in this high-risk area as it continues to meet the leadership commitment criterion through various actions. These include the President issuing (1) an executive order in May 2017 requiring federal agencies to take a variety of actions, including better managing their cybersecurity risks and coordinating to meet reporting requirements related to cybersecurity of federal networks

and critical infrastructure[19] and (2) a National Security Strategy in December 2017 citing cybersecurity as a national priority and identifying needed actions. Further, the administration issued a government-wide reform plan and reorganization recommendations in June 2018 with, among other things, proposals for solving the federal cybersecurity workforce shortage. Additionally, the administration released a National Cyber Strategy in September 2018 outlining activities such as securing critical infrastructure, federal networks, and associated information.

However, additional actions are needed. We have identified four major cybersecurity challenges facing the nation: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address the four major cybersecurity challenges, we identified 10 critical actions the federal government and other entities need to take. These critical actions include, for example, developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace; addressing cybersecurity workforce management challenges; and strengthening the federal role in protecting the cybersecurity of critical infrastructure (see figure 3).

[19]Executive Order 13,800, 82 Fed. Reg. 22,391 (May 16, 2017).

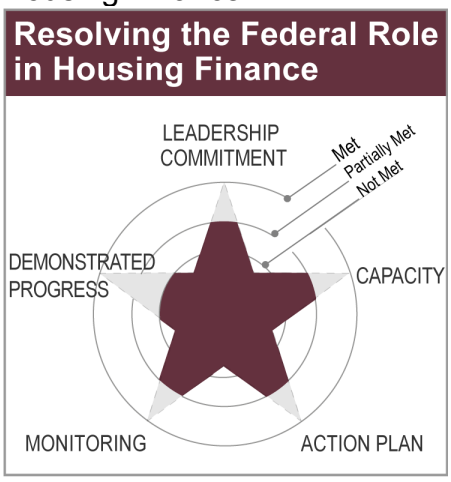
**Figure 3: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges**




Source: GAO analysis. | GAO-19-157SP

Until these shortcomings are addressed, federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist. See page 178 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Resolving the Federal Role in Housing Finance




Source: GAO analysis. | GAO-19-157SP

The expanded federal role in housing finance that began during the 2007–2009 financial crisis has substantially increased the government's exposure to potential mortgage losses. Federally supported mortgages include those backed by the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac)—collectively, the enterprises—which the Federal Housing Finance Agency (FHFA) placed into government conservatorships in 2008. Federal support also occurs through Federal Housing Administration (FHA) mortgage insurance and Government National Mortgage Association (Ginnie Mae) guarantees on mortgage-backed securities. The substantial financial assistance the enterprises required during and after the crisis, coupled with the large fiscal exposure they and other federal mortgage entities represent today, underscore the need to reform the federal role in housing finance.

Delay in resolving the federal role in housing finance poses considerable risks. Through the enterprises, FHA, and Ginnie Mae, the federal government is exposed to potential losses on several trillion dollars in mortgage debt. A severe economic downturn could trigger significant taxpayer assistance to one or more of these entities.

Congress and federal agencies have taken some steps to facilitate the transition to a revised federal role, such as holding hearings, introducing legislation, issuing regulations, and developing market monitoring tools. For example, in 2013 and 2014, housing and regulatory agencies finalized rules designed to prevent a recurrence of risky practices in originating and securing mortgages that contributed to the financial crisis. Additionally, FHFA and the Consumer Financial Protection Bureau have developed a representative database of mortgage information that could be useful for examining the effect of mortgage market reforms. However, overall progress on resolving the federal role will be difficult to achieve until Congress provides further direction by enacting changes to the housing finance system.

Several issues contribute to the risks facing federal housing finance, including the following:

- More than 10 years after entering federal conservatorships, the enterprises' futures remain uncertain and billions of taxpayer dollars remain at risk. Under agreements with the Department of the Treasury (Treasury), the enterprises have received $191.4 billion in capital support as of the end of fiscal year 2018 and have paid dividends to the department exceeding that amount. If they were to incur major additional losses, they would draw required amounts from their remaining $254.1 billion in Treasury commitments. In addition, prolonged conservatorships could hinder development of the broader mortgage securities market by creating uncertainty and crowding out private investment.
- Nonbanks (lenders and loan servicers that are not depository institutions) have played an increasingly large role in the mortgage market in recent years. While nonbanks have helped provide access to mortgage credit, they also may pose additional risks, in part because they are not federally regulated for safety and soundness. However, FHFA lacks statutory authority to examine nonbank mortgage servicers and other third parties who do business with and pose potential risks to the enterprises.
- The statutory 2 percent capital requirement for FHA's $1.26 trillion mortgage insurance fund is not based on a specified risk threshold, such as the economic conditions the fund would be expected to withstand. As a result, it may not provide an adequate financial cushion under scenarios in which Congress may anticipate the fund would be self-sufficient. During the last housing downturn, the fund's capital ratio fell below the required level and remained there for 6 consecutive years. At the end of fiscal year 2013, the fund required supplemental funds—about $1.7 billion—for the first time in its history.

Six of our federal housing recommendations remain open, including those we made in June 2015 on assessing the effects of mortgage reforms already in place.

Further, as we previously recommended in November 2016 and January 2019, Congress should consider housing finance reform legislation that:

- establishes objectives for the future federal role in housing finance, including the role and structure of the enterprises within the housing finance system;
- provides a transition plan to a reformed system that enables the enterprises to exit federal conservatorship; and

- addresses all relevant federal entities, including FHA and Ginnie Mae.

As we recommended in March 2016 and November 2017, respectively, Congress also should consider granting FHFA explicit authority to examine nonbank servicers and other third parties that do business with the enterprises, and specifying the economic conditions FHA's insurance fund would be expected to withstand without a substantial risk of requiring supplemental funds. See page 95 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

Due to the significance and risk associated with Resolving the Federal Role in Housing Finance, we are separating it from the high-risk area of Modernizing the U.S. Financial Regulatory System. These areas were combined in our 2017 High-Risk report. See page 95 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Pension Benefit Guaranty Corporation Insurance Programs


Source: GAO analysis. | GAO-19-157SP

The Pension Benefit Guaranty Corporation (PBGC) is responsible for insuring the defined benefit pension plans for nearly 37 million American workers and retirees, who participate in about 24,800 private sector plans. PBGC faces an uncertain financial future due, in part, to a long-term decline in the number of traditional defined benefit plans and the collective financial risk of the many underfunded pension plans that PBGC insures.

PBGC's financial portfolio is one of the largest of all federal government corporations. While PBGC's single employer program had a net surplus of about $2.4 billion at the end of fiscal year 2018, its multiemployer program had a net deficit of about $54 billion—or a combined net accumulated financial deficit of over $51 billion. Its deficit has increased by nearly 45 percent since fiscal year 2013. PBGC has estimated that, without additional funding, its multiemployer insurance program will likely be exhausted by 2025 as a result of current and projected pension plan insolvencies. The agency's single-employer insurance program is also at risk due to the continuing decline of traditional defined benefit pension plans, as well as premiums that are not well aligned to the financial risk presented by the plans it insures.

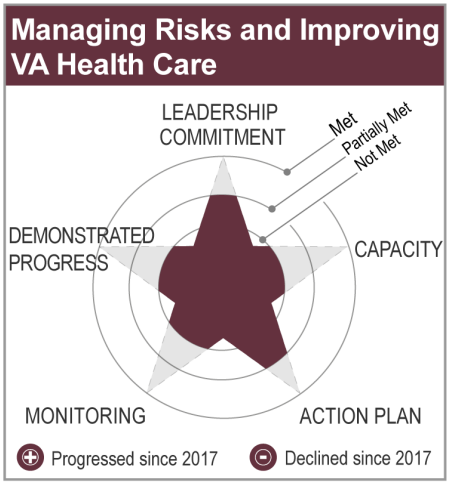
While Congress and PBGC have taken significant and positive steps to strengthen the agency in the past 5 years, challenges related to PBGC's funding and governance structure remain. Congress established a temporary Joint Select Committee on multiemployer pension plans in

2018—with the goal of improving the solvency of the multiemployer program. However, the committee did not release draft legislation. Addressing the significant financial risk and governance challenges that PBGC faces will require additional congressional action.

Over the years since we added PBGC to the High-Risk List, we have suggested a number of matters for congressional consideration, including: (1) authorizing a redesign of PBGC's single employer program premium structure to better align premium rates with sponsor risk; (2) adopting additional changes to PBGC's governance structure—in particular, expanding the composition of its board of directors; (3) strengthening funding requirements for plan sponsors as appropriate given national economic conditions; (4) working with PBGC to develop a strategy for funding PBGC claims over the long term as the defined benefit pension system continues to decline; and (5) enacting additional structural reforms to reinforce and stabilize the multiemployer system, and balance the needs and potential sacrifices of contributing employers, participants, and the federal government.

Absent additional steps to improve PBGC's finances, the long-term financial stability of the agency remains uncertain, and the retirement benefits of millions of American workers and retirees could be at risk of dramatic reductions. See page 267 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Managing Risks and Improving VA Health Care




Source: GAO analysis. | GAO-19-157SP

VA operates one of the largest health care delivery systems in the nation through its Veterans Health Administration (VHA), with 172 medical centers and more than 1,000 outpatient facilities organized into regional networks. VA has faced a growing demand by veterans for its health care services—due, in part, to the needs of an aging veteran population—and that trend is expected to continue. The total number of veterans enrolled in VA's health care system rose from 7.9 million to more than 9 million from fiscal year 2006 through fiscal year 2017. Over that same period, VHA's total budgetary resources have more than doubled, from $37.8 billion in fiscal year 2006 to $92.3 billion in fiscal year 2017.

Given the importance of VHA's mission, coupled with its lack of progress in addressing its high-risk designation, we continue to be concerned about VHA's ability to ensure its resources are being used effectively and efficiently to improve veterans' timely access to safe and high-quality health care. We have identified five areas of concern: (1) ambiguous policies and inconsistent processes; (2) inadequate oversight and

accountability; (3) IT challenges; (4) inadequate training for VA staff; and (5) unclear resource needs and allocation priorities. VHA has begun to address each of these areas but, prior to Secretary Robert Wilkie's July 2018 confirmation, its efforts were impeded by leadership instability. Since taking office, Secretary Wilkie has demonstrated his commitment to addressing the department's high-risk designation by, among other things, creating an office to direct an integrated, focused high-risk approach and communicating to VA leaders the importance of addressing our recommendations.

While VHA completed root cause analyses for each area of concern and developed an action plan in response, the plan lacks milestones and metrics needed to effectively monitor its implementation and demonstrate progress made in addressing the high-risk designation. Additionally, many of VHA's capacity-building initiatives are either in the initial stages of development or are lacking necessary funding and resources. As such, VHA has not made sufficient progress since our 2017 update to improve its overall ratings, as two high-risk criteria remain partially met and three criteria remain unmet.

We remain concerned about VHA's ability to oversee its programs, hold its workforce accountable, and avoid ambiguous policies and inconsistent processes that jeopardize its ability to provide safe, high-quality care to veterans:

- In November 2017, we reported that, due in part to misinterpretation or lack of awareness of VHA policy, VA medical center officials did not always document or conduct timely required reviews of providers when allegations were made against them. As a result, we concluded that VA medical center officials may have lacked necessary information to reasonably ensure that their providers were competent to provide safe, high-quality care to veterans and to grant approvals about these providers' privileges to perform specific clinical services at VA medical centers. We made four recommendations related to this and other findings, all of which remain open.
- In June 2018, we reported that VHA could not systematically monitor the timeliness of veterans' access to Veterans Choice Program (VCP) care because it lacked complete, reliable data to do so. We also found that veterans, who were referred to the VCP for routine care because health care services were not available in a timely manner, could potentially wait for care up to 70 calendar days if the maximum amount of time allowed by VA processes is used. This wait time exceeds the statutory requirement that veterans receive VCP care

within 30 days of the dates their VA health care providers indicated they should receive appointments, or if no such date existed, within 30 days of the veteran's preferred date. We made 10 recommendations related to this and other findings, all of which remain open.

- Similarly, in July 2018, we reported that VA collected data related to employee misconduct and disciplinary actions, but data fragmentation and reliability issues impeded department-wide analysis of those data. Additionally, we found that VA did not consistently ensure that allegations of misconduct involving senior officials were reviewed according to its investigative standards or ensure these officials were held accountable. We made 16 recommendations related to this and other findings, all of which remain open.
- In November 2018, we reported that VHA's suicide prevention media outreach activities declined in recent years due to leadership turnover and reorganization. Additionally, we found that VHA did not assign key leadership responsibilities or establish clear lines of reporting for its suicide prevention media outreach campaign, which hindered its ability to oversee the campaign. Consequently, we concluded that VHA may not be maximizing its reach with suicide prevention media content to veterans, especially those who are at-risk. This is inconsistent with VHA's efforts to reduce veteran suicides, which is VA's highest clinical priority. We made two recommendations related to this and other findings, both of which remain open.

VA needs to further develop its capacity-building initiatives and establish metrics to monitor and measure its progress addressing the high-risk areas of concern. It is also important that our recommendations continue to be implemented. The department has implemented 209 of the 353 recommendations related to VA health care that we made from January 1, 2010 through December 2018, but more than 125 recommendations remain open as of December 2018. This includes 17 that are older than 3 years. In addition to addressing our recommendations, VA needs to make systemic change to department management and oversight in order to fully address the high-risk issues and improve the health care provided to our nation's veterans.

See page 275 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Strategic Human Capital Management


Source: GAO analysis. | GAO-19-157SP

Mission-critical skills gaps both within federal agencies and across the federal workforce impede the government from cost-effectively serving the public and achieving results. For example, the difficulties in recruiting and retaining skilled health care providers and human resource staff at VHA's medical centers make it difficult to meet the health care needs of more than 9 million veterans. As a result, VHA's 168 medical centers have large staffing shortages, including physicians, registered nurses, physician assistants, psychologists, physical therapists, as well as human resource specialists and assistants.

OPM continues to demonstrate top leadership commitment through its numerous efforts to assist agencies' in addressing mission-critical skills gaps within their workforces. This includes providing guidance, training and on-going support for agencies on the use of comprehensive data analytic methods for identifying skills gaps and the development of strategies to address these gaps. However, since we first added strategic human capital management to our High-Risk List in 2001, we have reported on the need for agencies to address their workforce skills gaps.

As of December 2018, OPM had not fully implemented 29 of our recommendations made since 2012 relating to this high-risk area. Staffing shortages and the lack of skills among current staff not only affect individual agencies but also cut across the entire federal workforce in areas such as cybersecurity and acquisition management. Skills gaps caused by insufficient number of staff, inadequate workforce planning, and a lack of training in critical skills are contributing to our designating other areas as high-risk.

As table 5 shows, of the 34 other high-risk areas covered in this report, skills gaps played a significant role in 16 of the areas.

**Table 5: Skills Gaps Related to High-Risk Areas**

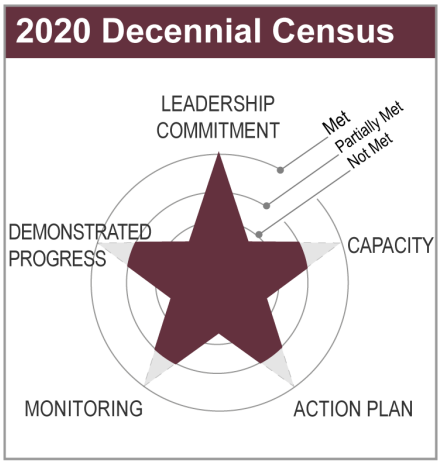
| High-risk area | Examples of skills gaps and causes |
|---|---|
| **2020 Decennial Census** | **Staffing:** Lack of staff to oversee the $886 million contract for integrating the Information Technology (IT) systems needed to conduct the 2020 Census. |
| **Strengthening DHS Management Functions** | **Workforce Planning:** Lack of guidance on how to identify critical cybersecurity and acquisition skills needed to support its new IT delivery model.<br>**Training:** Insufficient technical skills to support its biometric identification services program. |
| **DOD Business Systems Modernization** | **Workforce Planning:** Incomplete assessment of the extent to which DOD personnel meet IT management knowledge and skill requirements.<br>**Staffing:** Slow and inefficient hiring processes have led to challenges in recruiting and retaining qualified chief information officers (CIO) and IT personnel.<br>**Training:** Statutorily required guidance and training for cross-functional team members and presidential appointees not completed. |
| **DOD Financial Management** | **Staffing:** Financial management staff remains insufficient in number, qualifications, and expertise. |
| **DOD Contract Management** | **Staffing:** Challenges in recruiting talent for acquisition management. |
| **DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management** | **Workforce Planning:** Unmet critical staffing needs and evidence that the agency is understaffed across all functions.<br>**Staffing:** Competing agency priorities and limited hiring have contributed to critical staff shortages to manage and oversee strategic materials programs. |
| **U.S. Government's Environmental Liability** | **Workforce Planning:** Lack of information to evaluate overall project and program performance, including number of staff and skills needed to meet its environmental management cleanup mission. |
| **Improving Federal Management of Programs that Serve Tribes and Their Members** | **Staffing:** Lack of expert staff to review proposals for wind and solar projects, or petroleum engineers to review oil and gas proposals. Additionally, shortages of health care providers, including physicians, nurses, midwives, dentists, and pharmacists.<br>**Training:** Limited funding and lack of a safety training plan contributed to incomplete training to protect Bureau of Indian Education schools. |
| **Management of Federal Oil and Gas Resources** | **Workforce Planning:** Lacks plan for identifying key oil and gas positions and their respective technical competencies. No evaluation of the effectiveness of its recruitment and retention incentives as well as its student loan repayment program.<br>**Training:** No evaluation of its training needs, training effectiveness, or opportunities for its bureaus to share training resources. |
| **NASA Acquisition Management** | **Staffing and Skills:** Lacks staff or staff with skills in the areas of avionics, flight software, systems engineering, business management, software development for certain acquisition projects, as well as gaps in areas such as cost estimating and earned value management capabilities. |
| **Protecting Public Health Through Enhanced Oversight of Medical Products** | **Staffing:** At times, significant gaps in staffing still remain during the time staff complete necessary processes to be stationed overseas. |

| High-risk area | Examples of skills gaps and causes |
|---|---|
| **Improving and Modernizing Federal Disability Programs** | **Staffing:** SSA's disability appeals plan calls for increased hiring to reduce disability appeals backlogs and improve timeliness, and VA has not completed hiring and planning efforts to ensure it has the capacity to comprehensively update its disability eligibility criteria. |
| **VA Acquisition Management** | **Training:** Lack of training for contracting officers. |
| **Managing Risks and Improving VA Health Care** | **Workforce Planning:** No annual tracking and reviewing of data related to IT skills needed in the future.<br>**Staffing:** Insufficient number of community care staff and medical support assistants.<br>**Training:** No assessment of the training needs or monitoring of completed training for patient advocate positions. |
| **Ensuring the Cybersecurity of the Nation** | **Staffing and Training:** The administration's June 2018 government reform plan includes recommendations for solving the federal cybersecurity workforce shortage, including prioritizing and accelerating efforts to reform how the federal government recruits, evaluates, selects, pays, and places cyber talent. |
| **Improving the Management of IT Acquisitions and Operations** | **Workforce Planning:** None of the 24 major federal agencies had IT management policies that fully addressed the role of their CIOs. The majority of the agencies minimally addressed or did not address their CIO's role in assessing agency IT workforce needs, and developing strategies and plans for meeting those needs. |

Source: GAO analysis. | GAO-19-157SP

Over the years since we added this area to our High-Risk List, in addition to recommendations to address critical skills gaps in individual high-risk areas, we have made numerous recommendations to OPM related to this high-risk issue, 29 of which remain open. Agencies also need to take action to address mission-critical skills gaps within their own workforces – a root cause of many high-risk areas. See page 75 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## 2020 Decennial Census




Source: GAO analysis. | GAO-19-157SP

The 2010 Census was the costliest in history at about $12.3 billion; as of October 2017, the 2020 Census is projected to cost about $15.6 billion, a 27 percent increase. For the 2020 Census, the U.S. Census Bureau (Bureau) plans to implement several innovations, including new IT systems. Implementing these innovations, along with other challenges, puts the Bureau's ability to conduct a cost-effective census at risk.

The decennial census is mandated by the U.S. Constitution and provides vital data for the nation. Census data are used, among other purposes, to apportion seats in the Congress and allocate billions of dollars in federal assistance to state and local governments. To ensure its success, this complicated and costly undertaking requires careful planning, risk management, and oversight. Census activities, some of which are new for the 2020 cycle, must be carried out on schedule to deliver the state apportionment counts to the President by December 31, 2020.

The Bureau and the Department of Commerce (Commerce) have strengthened leadership commitment with executive-level oversight of the 2020 Census by holding regular meetings on the status of IT systems and other risk areas. In addition, in 2017 Commerce designated a team to assist senior Bureau management with cost estimation challenges. These examples demonstrate both the Bureau's and Commerce's strong leadership commitment to implementing the 2020 Census.

One of the Bureau's major challenges is to control any further cost growth and develop cost estimates that are reliable and reflect best practices for the 2020 Census. According to the Bureau, the total cost of the 2020 Census is now estimated to be approximately $15.6 billion, more than $3 billion higher than previously estimated by the Bureau. The higher estimated life-cycle cost is due, in part, to the Bureau's failure to previously include all cost associated with the decennial census.

The Bureau's schedule for developing IT systems has experienced delays that have compressed the time available for system testing, integration testing, and security assessments. These schedule delays have contributed to systems experiencing problems after deployment, as well as cybersecurity challenges. For example, as of December 2018, the Bureau had identified nearly 1,100 system security weaknesses that needed to be addressed. Continued schedule management challenges may compress the time available for the remaining system testing and security assessments, and increase the risk that deployed systems will either not function as intended, have security vulnerabilities, or both.

As of January 2019, 30 of our recommendations related to this high-risk area had not been implemented. To make continued progress, the Bureau needs to ensure that its approach to strategic planning, IT management, cybersecurity, human capital management, internal collaboration, knowledge sharing, as well as risk and change management are all aligned toward delivering more cost-effective outcomes. Among other things, the Bureau needs to ensure cost growth is controlled and that the development and testing of key systems is completed and fully integrated with all census operations before the 2020 Census. In addition, the Bureau needs to address cybersecurity weaknesses in a timely manner and ensure that security risks are at an acceptable level before systems are deployed. See page 134 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

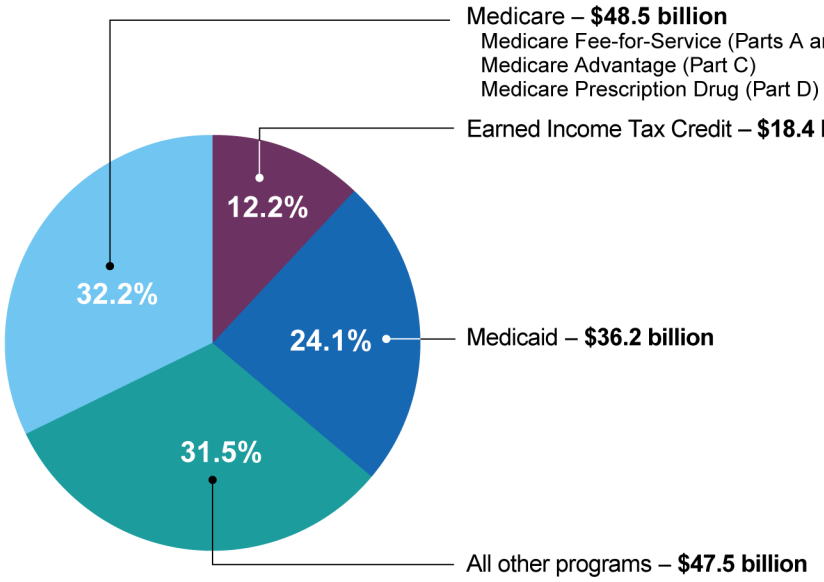
## Medicare, Medicaid, and Earned Income Tax Credit Improper Payments

An improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. Reducing improper payments—such as payments to ineligible recipients or duplicate payments—is critical to safeguarding federal funds. However, the federal government has consistently been unable to determine the full extent of improper payments and reasonably assure that appropriate actions are taken to reduce them.

Since 2003—when certain agencies were required by statute to begin reporting improper payments—cumulative improper payment estimates have totaled about $1.5 trillion. As shown in figure 4, for fiscal year 2018, federal entities estimated about $151 billion in improper payments. Medicare and Medicaid improper payments and the Earned Income Tax Credit (EITC) improper payments—a part of the Enforcement of Tax Laws high-risk area—accounted for about 68.5 percent of this total.

Federal spending for Medicare programs and Medicaid is expected to significantly increase in the coming years, so it is especially critical to take appropriate measures to reduce improper payments in these programs. Internal Revenue Service estimates also show that the EITC has consistently had a high improper payment rate. OMB has designated Medicare programs, Medicaid, and EITC as high-priority programs for improper payments, indicating they are amongst the highest-risk programs where the government can achieve the greatest return on investment for the taxpayer by ensuring that improper payments are eliminated.

**Figure 4: Improper Payment Estimates Were Concentrated in Three Areas in Fiscal Year 2018**




Source: GAO analysis of agencies' fiscal year 2018 data. | GAO-19-157SP

Our work has identified a number of strategic and specific actions agencies can take to reduce improper payments, which could yield significant savings, and help ensure that taxpayer funds are adequately safeguarded. Continued agency attention is needed to (1) identify susceptible programs, (2) develop reliable methodologies for estimating improper payments, (3) report as required by statute, and (4) implement effective corrective actions based on root cause analysis. Absent such continued efforts, the federal government cannot be assured that taxpayer funds are adequately safeguarded.

See pages 241, 250, and 235 of the report (respectively) for additional detail on the Medicare Program & Improper Payments, Strengthening Medicaid Program Integrity, and Enforcement of Tax Laws high-risk areas, including more details on actions that need to be taken.

## Enforcement of Tax Laws


Source: GAO analysis. | GAO-19-157SP

The Internal Revenue Service (IRS) continues to face two pressing challenges in enforcing tax laws: addressing the tax gap—amounting to hundreds of billions of dollars each year when some taxpayers fail to pay the taxes that they owe—and combatting identity theft (IDT) refund fraud. Enforcement of Tax Laws has been on GAO's high risk list since 1990.

IRS enforcement of tax laws helps fund the U.S. government by collecting revenue from noncompliant taxpayers and, perhaps more importantly, promoting voluntary compliance by giving taxpayers confidence that others are paying their fair share. In 2016, IRS estimated that the average annual net tax gap, the difference between taxes owed and taxes paid on time, was $406 billion, on average, for tax years 2008-2010.

While IRS continues to demonstrate top leadership support to address the tax gap, IRS's capacity to implement new initiatives and improve ongoing enforcement and taxpayer service programs remains a challenge. For example, IRS's strategic plan includes a goal to facilitate voluntary compliance and deter noncompliance that could address the tax gap. However, IRS could do more to identify specific efforts for improving compliance in its strategic plan, measure the effects of compliance programs—such as those used for large partnerships—and develop specific quantitative goals to reduce the tax gap. Such efforts would help IRS make more effective use of its resources and gauge the success of its strategies.

The second challenge facing IRS is IDT refund fraud, which occurs when an identity thief files a fraudulent tax return using a legitimate taxpayer's identifying information and claims a refund. IRS estimates that at least $12.2 billion in individual IDT tax refund fraud was attempted in 2016, of which it prevented at least $10.5 billion (86 percent). Of the amount attempted, IRS estimated that at least $1.6 billion (14 percent) was paid.

IRS's ability to combat IDT fraud continues to be challenged as more personally identifiable information has become readily available as a result of large-scale cyberattacks on various entities. This makes it more difficult for IRS to distinguish between fraudsters and legitimate taxpayers.

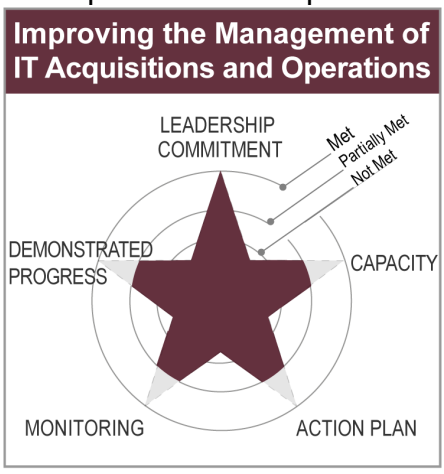
While IRS has demonstrated some progress by developing tools and programs to further detect and prevent IDT refund fraud, it has not completed updating its authentication procedures to be in compliance with new government standards. As a result, IRS may be missing an

opportunity to implement the most secure, robust technologies to protect taxpayers.

As of December 2018, 189 GAO recommendations related to this high-risk area had not been implemented. To make continued progress on closing the tax gap, IRS needs to re-establish goals for improving voluntary compliance and develop and document a strategy that outlines how it will use its data to help address this issue. Reducing the tax gap will also require targeted legislative actions, including additional third-party information reporting, enhanced electronic filing, expanded math error authority (also referred to as correctible error authority), and paid preparer regulation. To help stay on top of IDT refund fraud, IRS should develop a comprehensive process to evaluate alternative options for improving taxpayer authentication. Given that IDT refund fraud continues to be a challenge, targeted legislative action, such as requiring a scannable code on returns prepared electronically but filed on paper could help IRS address such fraud.

See page 235 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

## Improving the Management of IT Acquisitions and Operations




Source: GAO analysis. | GAO-19-157SP

The federal government currently invests more than $90 billion annually in IT, and OMB has implemented several key initiatives intended to help better manage this investment. Additionally, enactment of FITARA, in conjunction with greater attention paid to the acquisition and operation of IT, has helped further improve the government-wide management of this significant annual investment.[20] OMB's current level of top leadership support and commitment to ensure that agencies successfully execute its guidance on implementing FITARA and related IT initiatives has helped this high-risk area meet the leadership commitment high-risk criteria.

Additional positive government-wide actions have enabled this high-risk area to partially meet the four remaining high-risk criteria. For example, OMB has established an IT Dashboard—a public website that provides detailed information on major IT investments at 26 federal agencies—and agencies' data center consolidation efforts have resulted in a total savings of slightly more than 80 percent of the agencies' planned $5.7 billion in savings since 2011. However, major federal agencies have yet to fully

[20]FITARA was enacted into law as part of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, §§ 831-837, 128 Stat. 3292, 3438-3450 (2014).

address the requirements of FITARA and realize billions of dollars in planned or possible savings and improved government performance through more efficient budgeting and management of IT.

As government-wide spending on IT increases every year, the need for appropriate stewardship of that investment increases as well. However, OMB and federal agencies have not made significant progress since 2017 in taking the steps needed to improve how these financial resources are budgeted and utilized. While OMB has continued to demonstrate its leadership commitment through guidance and sponsorship of key initiatives, agencies still have not fully implemented all requirements of FITARA, such as putting into place authorities the law requires for chief information officers (CIO). Additionally, while the President's Management Agenda has a goal to improve IT spending transparency, agencies are underreporting IT contract obligations by billions of dollars. OMB and the agencies also have not yet implemented hundreds of our recommendations on improving shortcomings in IT acquisitions and operations.

In an August 2018 review of the 24 federal agencies covered by FITARA, none had IT management policies that fully addressed the role of their CIOs consistent with federal laws and guidance. Specifically, the majority of the agencies only minimally addressed, or did not address, their CIO's role in assessing agency IT workforce needs and developing strategies and plans for meeting those needs. Correspondingly, the majority of the 24 CIOs acknowledged that they were not fully effective at implementing IT management responsibilities, such as IT strategic planning and investment management.

Further, in January 2018, we reported that the majority of 22 agencies did not identify all of their IT acquisition contracts, totaling about $4.5 billion in IT-related contract obligations beyond those reported by agencies. In addition, in November 2018 we reported that four selected agencies lacked quality assurance processes for ensuring that billions of dollars requested in their IT budgets were informed by reliable cost information. Until agencies properly identify IT contracts and establish processes for ensuring the quality of cost data used to inform their budgets, agency CIOs are at risk of not having appropriate oversight of IT acquisitions and may lack adequate transparency into IT spending to make informed budget decisions.

As of December 2018, OMB and federal agencies had fully implemented only 59 percent of the recommendations we have made since fiscal year

2010 to address shortcomings in IT acquisitions and operations. OMB and agencies should work toward implementing our remaining 456 open recommendations related to this high-risk area. These remaining recommendations include 12 priority recommendations to agencies to, among other things, report all data center consolidation cost savings to OMB, plan to modernize or replace obsolete systems as needed, and improve their implementation of PortfolioStat—an initiative that is to consolidate and eliminate duplicative systems.

OMB and agencies need to take additional actions to (1) implement at least 80 percent of our open recommendations related to the management of IT acquisitions and operations, (2) ensure that a minimum of 80 percent of the government's major IT acquisitions deliver functionality every 12 months, and (3) achieve at least 80 percent of the over $6 billion in planned PortfolioStat savings.

See page 123 of the report for additional detail on this high-risk area, including more details on actions that need to be taken.

Our high-risk program continues to be a top priority at GAO and we will maintain our emphasis on identifying high-risk issues across government and on providing recommendations and sustained attention to help address them, by working collaboratively with Congress, agency leaders, and OMB. As part of this effort, we hope to continue to participate in regular meetings with the OMB Deputy Director for Management and with top agency leaders to discuss progress in addressing high-risk areas. Such efforts have been critical for the progress that has been made.

This high-risk update is intended to help inform the oversight agenda for the 116th Congress and to guide efforts of the administration and agencies to improve government performance and reduce waste and risks.

Thank you, Chairman Johnson, Ranking Member Peters, and Members of the Committee. This concludes my testimony. I would be pleased to answer any questions.

For further information on this testimony, please contact J. Christopher Mihm at (202) 512-6806 or MihmJ@gao.gov. Contact points for the individual high-risk areas are listed in the report and on our high-risk website. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

# Appendix I: Summaries of Selected High-Risk Areas

The following pages provide summaries of selected high-risk areas. These summaries are included in our High-Risk Report and are also available on our High-Risk List website, http://www.gao.gov/highrisk/overview.

# Strategic Human Capital Management

The Office of Personnel Management and federal agencies must continue developing the capacity to measure and address existing mission-critical skills gaps, and use workforce analytics to predict and mitigate future gaps so agencies can effectively carry out their missions.

**Why Area Is High Risk**

Mission-critical skills gaps both within federal agencies and across the federal workforce pose a high risk to the nation because they impede the government from cost-effectively serving the public and achieving results. This area was added to the High-Risk List in 2001.

We, along with OPM and individual agencies, have identified skills gaps in such government-wide occupations in the fields of science, technology, engineering, mathematics, cybersecurity, and acquisitions. Causes for these skills gaps vary; however, they often occur due to a shortfall in one or more talent management activities such as robust workforce planning or training. Additionally, the changing nature of federal work and the high percentage of employees eligible for retirement could produce gaps in leadership and institutional knowledge, and could threaten to aggravate the problems created from existing skills gaps. For example, 31.6 percent of permanent federal employees who were on board as of September 30, 2017, will be eligible to retire in the next five years with some agencies having particularly high levels of employees to retire.

Mission-critical skills gaps are a contributing factor in making other areas across the government high risk. Of the 34 other high-risk areas, skill gaps played a significant role in 16 areas, such as veterans' health care.

**Contact Information**

For additional information about this high-risk area, contact Robert Goldenkoff at (202)512-2757 or goldenkoffr@gao.gov or Yvonne D. Jones at (202) 512-2717 or jonesy@gao.gov.


Source: GAO analysis. | GAO-19-157SP

For this high-risk area, all five criteria remain unchanged since our previous report in 2017.

**Leadership commitment: met.** The Office of Personnel Management (OPM) continues to demonstrate top leadership commitment through its numerous efforts to assist agencies in addressing mission-critical skills gaps within their workforces. OPM's regulation on strategic human capital management, which took effect in April 2017, requires executive branch agencies to issue human capital operating plans that, in part, must describe the agencies' skills gaps and the strategies to be used for closing these gaps. OPM has provided guidance, training, and on-going support for agencies on the use of comprehensive data analytic methods for identifying skills gaps and the development of strategies to address these gaps. Additionally, the Director of OPM uses the Chief Human Capital Officers (CHCO) Council's quarterly meetings to review and discuss agency data on the closure of agency-specific skills gaps.

**Capacity: partially met.** OPM and the CHCO Council continue supporting the efforts of the Federal Agency Skills Teams (FAST), which consist of occupational leaders and CHCO representatives who are responsible for setting goals for closing skills gaps and using measureable targets and appropriate metrics. OPM staff meet quarterly with FASTs to provide guidance on the development of action plans and use of OPM's multi-factor model, a methodology for identifying skills gaps. In mid-2019, OPM plans to launch an automated version of the multi-factor model to facilitate and promote its use among FASTs.

**Action plan: partially met.** On a quarterly basis, OPM staff review and provide feedback to FASTs on the content of their action plans, such as the identification of the root causes for the skills gap, assignment of roles and responsibilities for implementing strategies, and the creation of outcome-oriented performance metrics. Additionally, OPM staff stated that they continue to train FAST members on applying OPM's multi-factor model, developing a sound action plan, and identifying strategies for addressing identified skills gaps.

**Monitoring: partially met.** On a quarterly basis, OPM provides to agencies' management and FASTs a data dashboard of 12 metrics which gives a snapshot of agencies' progress on closing identified skills gaps. In March 2019, OPM plans to begin a "midterm" review of agencies' efforts to mitigate skills gaps by issuing a memo to agencies asking for the status on their specific skills gaps and a description of challenges encountered during their efforts.

**Demonstrated progress: not met.** On the one hand, OPM has, among other actions, issued a regulation and developed tools and processes that could help agencies better identify and address current and newly emerging skills gaps. Additionally, senior agency leaders are required to meet annually with OPM officials to hold high-level, data-driven discussions on agencies' progress towards meeting their human capital goals.

On the other hand, OPM needs to ensure that individual agencies implement guidance, tools, and training, and fully develop and implement effective strategies to mitigate and close skills gaps within their own workforces. For instance, the inability of the Veterans Health Administration's human resource staff to implement an effective recruitment strategy has affected the ability of its medical centers to maintain an adequate team of medical professionals to meet veterans' health care needs.

Agencies' critical skills gaps contributed to 16 other high-risk areas and are noted throughout this report. They include 2020 Decennial Census, Strengthening DHS Management Functions, DOD Business Systems Modernization, DOD Financial Management, DOD Contract Management, DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management, U.S. Government's Environmental Liability, Improving Federal Management of Programs that Serve Tribes and Their Members, Management of Federal Oil and Gas Resources, NASA Acquisition Management, Protecting Public Health through Enhanced Oversight of Medical Products, Improving and Modernizing Federal Disability Programs, VA Acquisition Management, Managing Risks and Improving VA Health Care, Ensuring the Cybersecurity of the Nation, and Improving the Management of IT Acquisitions and Operations.

## What Remains to Be Done

Over the years since we added this area to our High-Risk List, in addition to recommendations to address critical skills gaps in individual high-risk areas, we have made numerous recommendations to OPM related to this high-risk issue, 29 of which remain open. OPM needs to fully address the recommendations in our January 2015 report which call on the Director of OPM to make more strategic use of government workforce data to build a predictive capacity for identifying and mitigating emerging skills gaps

across government. Our January 2015 report also recommended that OPM work with agency CHCOs to bolster the ability of agencies to assess workforce competencies by sharing competency surveys, lessons learned, and other tools and resources. Agencies also need to take action to address mission-critical skills gaps within their own workforces—a significant factor contributing to many high-risk areas.

## Related GAO Products

*Embassy Construction: Pace is Slower Than Projected, and State Could Make Program Improvements.* GAO-18-653. Washington, D.C.: September 25, 2018.

*Tax Administration: Opportunities Exist to Improve Monitoring and Transparency of Appeal Resolution Timeliness.* GAO-18-659. Washington, D.C.: September 21, 2018.

*Information Technology: IRS Needs to Take Actions to Address Significant Risks to Tax Processing.* GAO-18-298. Washington, D.C.: June 28, 2018.

*Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*. GAO-18-466. Washington, D.C.: June 14, 2018.

*Defense Acquisition Workforce: Opportunities Exist to Improve Practices for Developing Program Managers*. GAO-18-217. Washington, D.C.: February 15, 2018.

*Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*. GAO-18-175. Washington, D.C.: February 6, 2018.

*Bureau of Prisons: Better Planning and Evaluation Could Help Ensure Effective Use of Retention Incentives*. GAO-18-147. Washington, D.C.: December 7, 2017.

*National Weather Service: Actions Have Been Taken to Fill Increasing Vacancies, but Opportunities Exist to Improve and Evaluate Hiring*. GAO-17-364. Washington, D.C.: May 24, 2017.

*Strategic Human Capital Management: NRC Could Better Manage the Size and Composition of Its Workforce by Further Incorporating Leading Practices.* GAO-17-233. Washington, D.C.: April 27, 2017.

*Veterans Health Administration: Actions Needed to Better Recruit and Retain Clinical and Administrative Staff*. GAO-17-475T. Washington, D.C.: March 22, 2017.

# Managing Federal Real Property

The federal government would save millions of dollars by disposing of unneeded buildings and reducing lease costs. Federal departments and agencies should also improve data reliability and federal facility security.

**Why Area Is High Risk**

The federal government's real estate portfolio is vast and diverse—including about 267,000 domestic buildings as of September 2016 that cost billions of dollars annually to operate and maintain. OMB and GSA both provide management support to agencies. OMB establishes federal policies and chairs the Federal Real Property Council. GSA provides space for federal tenants and collects data on real property.

Additionally, DHS has management-level responsibilities through the DHS-chaired Interagency Security Committee (ISC) that sets security standards, and its Federal Protective Service (FPS) protects about 9,000 federal buildings. Federal managers, however, rely on other agencies to reduce unneeded properties, produce reliable data, and follow Interagency Security Committee standards.

Since federal real property management was placed on the High-Risk List in 2003, the federal government has given high-level attention to this issue; however, federal agencies continue to face long-standing challenges, including: (1) effectively disposing of excess and underutilized property, (2) relying too heavily on leasing, (3) collecting reliable real property data for decision making, and (4) protecting federal facilities.

**Contact Information**

For additional information about this high-risk area, contact Lori Rectanus at rectanusl@gao.gov or (202) 512-2834


Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, overall, the five criteria remain unchanged although there was progress within some individual segments. Three agencies involved in managing, tracking, and protecting federal real property government-wide—Office of Management and Budget (OMB), General Services Administration (GSA), and Department of Homeland Security (DHS)—have made steady progress over multiple administrations in addressing federal real property challenges. However, momentum has slowed, due to delayed implementation of the Federal Assets Sale and Transfer Act of 2016 (FASTA) and decreased implementation of reforms by federal agencies. Over the years since we added this area to our High-Risk List, we have made numerous recommendations related to this high-risk issue, 40 of which were made since the last high-risk update in February 2017. As of December 2018, 63 recommendations are open

## Excess and Underutilized Property


Source: GAO analysis. | GAO-19-157SP

Ratings for this segment remain unchanged since our 2017 High-Risk Report.

**Leadership commitment: met.** In 2015, OMB implemented our recommendation to issue government-wide guidance—the National Strategy for the Efficient Use of the Real Property (National Strategy)—which identified actions to reduce the size of the federal real property portfolio by prioritizing consolidation, co-location, and disposal actions, consistent with the Reduce the Footprint policy that required agencies to set goals for reducing unneeded space. An OMB official said that the National Strategy and Reduce the Footprint Policy are still in place.

In 2016, FASTA established a 7-member civilian board to recommend unneeded federal buildings for disposal. However, the administration has not yet appointed a chair, a full board, or staff.

In 2018, the Administration released its plan on Delivering Government Solutions in the 21st Century. As part of this plan, the Administration proposed a series of improvements to streamline and accelerate the disposal of excess federal property. These improvements include reducing the number of steps needed to dispose of unneeded federal property and creating incentives for disposals by allowing agencies to retain the proceeds from sales.

**Capacity: partially met.** As noted in our 2017 high-risk update, OMB created the National Strategy and the Reduce the Footprint Policy to assist agencies, which represented positive steps. However, the National Strategy does not address the extent to which underlying challenges, such as budget limitations, impede agencies' abilities to dispose of or better use real property, nor does it offer guidance on how agencies can overcome these challenges. Once the board is appointed, FASTA has the potential to increase the federal government's capacity by establishing a process for identifying and disposing of unneeded federal buildings.

**Action plan: met.** We noted in 2017 that OMB had, through the Reduce the Footprint policy, established a government-wide action plan to (1) use property as efficiently as possible, and (2) reduce portfolios through annual reduction targets.

**Monitoring: partially met.** OMB and GSA monitor progress in meeting space reduction targets using the government-wide real property database called the Federal Real Property Profile (FRPP). However, the database is not yet sufficiently reliable to produce accurate results. The Department of Defense (DOD) has almost half of the federal government's buildings. However, OMB chose not to use DOD's real property data in reporting the 2017 results of the Reduce the Footprint policy—the most recent year for which data is available—because the data were not sufficiently reliable. We reported in 2018 that weaknesses in the quality of the DOD's real property data result, in part, because DOD has not developed a strategy to identify and address risks with accompanying time frames and performance metrics. Without such a strategy, DOD may miss the opportunity to reasonably ensure that the information needed for effective decision making by DOD, Congress, and other federal agencies is available to meet real property accountability and reporting objectives.

**Demonstrated progress: partially met.** The fiscal year 2016 results from Reduce the Footprint show progress with the federal government more than doubling its reduction goal. However, in fiscal year 2017, the federal government failed to reach the halfway point of its more modest reduction goal.

## What Remains to Be Done

As part of the reforms that OMB is considering, it should:

- identify alternative approaches to address underlying causes of real property problems and address the extent to which challenges impede progress, as we recommended in 2016; and
- refocus agency attention on meeting space reduction targets, as discussed.

Additionally, the Administration needs to appoint vacant FASTA board positions and hire staff.

# Costly Leasing


Source: GAO analysis. | GAO-19-157SP

The ratings for capacity and action plan improved since our 2017 High-Risk Report and the remaining three criteria remain unchanged.

**Leadership commitment: met.** OMB and GSA continue to take action to reduce costly leasing. For example, OMB proposed the creation of a capital revolving fund designed to facilitate ownership over operating leases for large-dollar buildings, although no action has been taken to implement it. An OMB staff member said that the legislative proposal to establish a capital fund was similar to an option we identified in a 2014 report. Additionally, GSA has developed a strategy to reduce leasing costs by a projected $4.7 billion by fiscal year 2023, through steps that include focusing resources on high-value lease renewals.

**Capacity: partially met.** GSA made improvements and now partially meets the capacity criterion. Specifically, GSA implemented our September 2013 recommendation to develop a strategy to increase ownership investments for a prioritized list of high-value leases. These leases are for properties where it would be less expensive in the long run to own. GSA plans to purchase at least one leased building in 2019. In addition, as noted in our 2017 high-risk update, GSA could potentially help tenant agencies save millions of dollars from some leases by loaning them funds to improve newly leased spaces instead of agencies financing these costs with private-sector owners at private-sector interest rates. While GSA officials agreed that doing so would save money in interest fees, it has not yet developed a legislative proposal to obtain the needed authority, as we recommended in 2016.

**Action plan: met.** GSA has made improvements and now meets the action plan criterion. GSA created an action plan to purchase buildings when it is more cost-effective than leasing by establishing criteria to rank and prioritize leased spaces that would benefit from federal ownership as

discussed above. Additionally, GSA is implementing strategies to better manage leases that include avoiding short-term extensions and identifying opportunities to enter into long-term and lower cost leases.

**Monitoring: partially met.** GSA continues to partially meet this criterion through implementation of the National Strategy, as noted in our 2017 high-risk update. However, GSA should also implement our recommendations to reduce the costs to tenants by exploring strategies to enhance competition for GSA leases and reducing unneeded fees.

Additionally, GSA has identified actions to better monitor leases at different points along the process in order to minimize the need to enter into short-term, costly lease extensions.

**Demonstrated progress: partially met.** GSA has made some progress in reducing the long-term costs of leasing by stemming the growth in leasing according to GSA data and committing to further reducing leasing costs. However, GSA must follow through on its plans to purchase leased buildings and reduce costs. GSA could also further reduce costs by loaning tenant agencies the funds needed to improve newly leased spaces but still needs to develop a legislative proposal to obtain authority to do so.

## What Remains to Be Done

GSA should develop a legislative proposal to obtain authority to loan agencies funds needed to improve newly leased spaces, as we recommended in 2016.

# Data Reliability


Source: GAO analysis. | GAO-19-157SP

Ratings for one criterion improved since our 2017 High-Risk Report and the other four criteria remain unchanged.

**Leadership commitment: met.** In December 2017, GSA continued efforts to improve data reliability by completing a major effort to make the Federal Real Property Profile (FRPP) public. Also, as we reported in our 2017 High-Risk Report, GSA issued its Federal Real Property Data Validation and Verification (V&V) Guidance in May 2016 and required agencies to address 13,257 data anomalies it found in fiscal year 2016 data.

**Capacity: met.** OMB and GSA continue to help agencies' increase their capacity to submit accurate data. For example, GSA revised certain data elements' definitions in 2016 and incorporated them in the 2018 FRPP Data Dictionary. In addition, OMB and GSA have further increased the

capacity of FRPP to act as a government-wide database since additional agencies are required to report.

**Action plan: met.** GSA has made progress by developing an action plan in 2017 for federal agencies to develop processes to assess, address, and track FRPP data quality. Specifically, this plan identifies data elements to appropriately indicate data quality, identifies best practices and other methods that help agencies measure and assess improvements, and enables federal agencies to develop performance metrics.

**Monitoring: partially met.** While GSA required agencies to research the anomalies it found in its V&V process, only some agencies have identified and committed to correct mistakes. Further, of the 13,257 anomalies GSA identified in the fiscal year 2016 data, agencies overall acknowledged that less than 8 percent of the anomalies (1,004 anomalies) represented erroneous data to be corrected, while indicating that the others were correct. Furthermore, some agencies acknowledged less than 1 percent of the anomalies represented erroneous data. In addition, we found in 2018 that DOD did not correct discrepancies identified by its own V&V process.

**Demonstrated progress: partially met.** While GSA and some agencies have taken action to correct data, serious data reliability challenges remain with some individual agencies that undermine the reliability of the FRPP. In 2018, we found that DOD's real property data continue to be inaccurate and incomplete, and that DOD lacks a plan for making the necessary improvements.

## What Remains to be Done

OMB and GSA should continue working with federal agencies to improve the reliability of their real property data through V&V efforts and encouraging agencies to implement action plans to better assess, address, and track data quality, as discussed in the above action plan. In particular, DOD should take steps to ensure that DOD improves the reliability of its real property data, as we recommended in 2018.

# Physical Security


Source: GAO analysis. | GAO-19-157SP

Ratings for this segment remain unchanged since our 2017 High-Risk Report.

**Leadership commitment: met.** DHS's Federal Protective Service (FPS) continues to take action to address our recommendations. The Interagency Security Committee (ISC), an organization chaired by DHS that sets standards for physical security for federal nonmilitary facilities, also continues to implement the updated Risk Management Process—a consolidated set of standards for physical security at federal facilities. In addition, in 2018, GSA, the Administrative Office of the U. S. Courts (AOUSC), the U.S. Marshals Service, and FPS implemented our 2017 recommendation to establish a national-level working forum for courthouse security, known as the Interagency Judicial Security Council.

**Capacity: partially met.** FPS has taken several actions to address identified physical security issues since our 2017 High-Risk Report. For example, in 2018 FPS improved its risk assessment tool to incorporate all necessary elements recommended by the ISC, which has now certified it. In 2018, FPS also addressed our recommendation related to improving training for instructors and identified actions to address our recommendations associated with tracking guard training. Finally, in 2018, FPS also implemented several actions associated with our recommendation to develop human capital-related performance measures to evaluate progress towards agency goals.

Some agencies may not have the capacity to conduct adequate risk assessments because their processes do not fully align with the ISC Risk Management Process. To improve their capacity, the U.S. Customs and Border Protection, Federal Aviation Administration, and the Department of Veterans' Affairs still need to complete an assessment of their policies against the ISC's standards in response to our 2017 and 2018 recommendations.

**Action plan: partially met.** In September 2018, FPS and GSA signed a memorandum of agreement (MOA) clarifying their respective roles and responsibilities for federal facility security. However, FPS, GSA, and the Department of Justice have not yet addressed our 2011 recommendation to address a number of courthouse security challenges. Specifically, FPS, the U.S. Marshals Service, AOUSC, and GSA are still working to finalize the draft MOA on courthouse security.

**Monitoring: partially met.** FPS continues to develop a system that will allow FPS to verify independently that FPS's contract guards are current on all training and certification requirements, and are taking steps to close

this recommendation as implemented. FPS expects that system to be in place in 2019. In 2018, we also found that actions were needed to better address various emerging security threats to federal facilities.

**Demonstrated progress: not met.** The federal government has not demonstrated progress to improve physical security. Although agencies have taken some actions, time is needed for agencies to demonstrate the results of these actions. Additionally, agencies need to complete other actions. For example, once FPS, the U.S. Marshals Service, AOUSC, and GSA sign their MOA on courthouse security, they will be able to better protect federal facilities. Further, once FPS fully implements its guard management system and it interacts with its training system, FPS will be able to obtain information to assess its guards' capability to address physical security risks across its portfolio.

## What Remains to be Done

To improve the physical security of federal buildings, the following steps are necessary:

- Clarify roles and responsibilities for the protection of federal facilities by finalizing the MOA for federal courthouse security between GSA, FPS, the U.S. Marshals, and AOUSC, as we recommended in 2011.
- FPS must validate training information being entered to ensure that guards are getting critical training, as we recommended in 2012.
- Implement our recommendations for agencies to improve their monitoring of collaborative efforts to protect federal facilities, as we recommended in 2015.
- Take actions to better address emerging security threats to federal facilities, as we recommended in 2018.

## Related GAO Products

*Federal Facility Security: Actions Needed to Better Address Various Emerging Threats*. GAO-19-32SU. Washington, D.C.: October 17, 2018.

*Defense Real Property: DOD Needs to Take Additional Actions to Improve Management of Its Inventory Data*. GAO-19-73. Washington, D.C.: November 13, 2018.

*Federal Buildings: More Consideration of Operations and Maintenance Costs Could Better Inform the Design Excellence Program*. GAO-18-420. Washington, D.C.: May 22, 2018.

*Federal Real Property: Agencies Make Some Use of Telework in Space Planning but Need Additional Guidance*. GAO-18-319. Washington, D.C.: March 22, 2018.

*Federal Buildings: Agencies Focus on Space Utilization As They Reduce Office and Warehouse Space*. GAO-18-304. Washington, D.C.: March 8, 2018.

*VA Facility Security: Policy Review and Improved Oversight Strategy Needed*. GAO-18-201. Washington, D.C.: January 11, 2018.

*Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk*. GAO-18-72. Washington, D.C.: October 26, 2017.

*Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners*. GAO-17-195. Washington, D.C.: January 3, 2017.

# USPS Financial Viability

Comprehensive legislative reform and additional cost-cutting are needed for the U.S. Postal Service (USPS) to achieve sustainable financial viability.

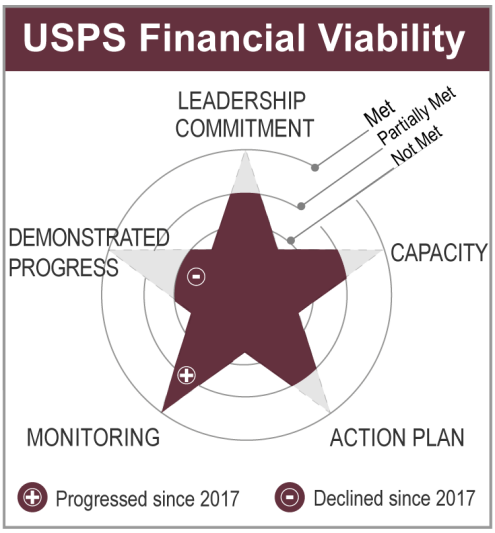
**Why Area Is High Risk**

USPS's financial viability has been on our High-Risk List due to the need for action to address USPS's poor financial condition. In July 2009, we reported that USPS's financial condition needed attention by Congress and the executive branch to achieve broad-based restructuring. Currently one open Matter for Congressional Consideration is related to this high-risk area.

USPS financial viability continues to be high-risk because USPS cannot fund its current level of services and financial obligations from its revenues. As an independent establishment in the executive branch, USPS has long been expected to provide affordable, quality, and universal postal service to all parts of the country while remaining self-financing. Specifically, USPS is expected to be financially self-sufficient by covering its expenses through revenues generated from the sale of its products and services. However, USPS is no longer able to do so. USPS's most profitable product—First-Class Mail—is expected to continue declining for the foreseeable future, and USPS faces increasing competition in its less profitable package shipping business. Meanwhile, key costs, such as compensation and benefits, are rising.

**Contact Information**

For additional information about this high-risk area, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.




Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, ratings for one criterion improved, one regressed, and three remain unchanged. The monitoring progress criterion is now met, but the demonstrated progress criterion regressed to not met.

Removal of USPS's financial viability from the High-Risk List would require fundamental changes. Both Congress and USPS need to act to put it on a sustainable financial footing. USPS has lost $69.0 billion over the past 11 fiscal years—including $3.9 billion in fiscal year 2018—and has budgeted for a $6.6 billion net loss in fiscal year 2019.

**Leadership commitment: partially met.** USPS continues to seek some legislative changes intended to improve its financial condition. For example, USPS has sought legislation that would integrate its retiree health program with Medicare, which would significantly reduce its total unfunded liabilities. USPS also has sought legislation that would require a rate increase for most mail. Further, USPS is seeking the elimination of the price cap that generally limits rate increases for most mail to the rate of inflation.

USPS has implemented limited initiatives to manage its labor costs, such as a small reduction to its workforce in fiscal year 2018 through attrition. USPS has stated that opportunities for further cost savings are limited under the existing legal framework and would do little to close its financial gap.

**Capacity: partially met.** USPS plans to increase capital spending in the coming decade to replace and modernize its infrastructure after years of reduced capital investment. For example, USPS plans to replace its aging fleet of delivery vehicles, which is intended to increase its capacity to deliver mail and packages in a more cost-efficient manner.

However, given the uncertainty of USPS's financial situation, the ability to carry out this spending may require tradeoffs with other commitments. USPS is only able to make capital investments and pay for its ongoing

operations by not making certain required federal payments to fund accrued retirement benefits.

**Action plan: partially met.** USPS issued its 5-year strategic plan for fiscal years 2017 to 2021 outlining its strategy for making progress towards financial viability, and developed annual performance plans that specify goals for each fiscal year. However, these plans fall short of maximizing what USPS can do within its existing authority to operate more efficiently and reduce its costs. For example, USPS has no plans to resume consolidating its processing facilities, recognizing that actions such as this would likely face stakeholder resistance.

**Monitoring: met.** USPS regularly monitors its financial condition and issues quarterly and independently-audited annual financial reports. The independent audits have consistently found that USPS's financial statements conform with U.S. generally accepted accounting principles and fairly present, in all material aspects, USPS's financial position at the end of each fiscal year, as well as the results of its operations and cash flows. USPS's quarterly and annual financial reports provide information on key trends and measures, such as (1) revenues and expenses; (2) unfunded liabilities; and (3) debt obligations. USPS publishes the reports on its public website and provides quarterly public webcasts on its financial results.

**Demonstrated progress: not met.** USPS's overall financial condition is deteriorating and unsustainable. The savings from USPS cost-reduction efforts have dwindled in recent years and although USPS has stated it will aggressively reduce costs within its control, USPS's plans will not achieve the kind of savings necessary to significantly reduce current operating costs. USPS expenses are now growing faster than its revenues, in part due to rising compensation and benefits costs combined with continuing declines in First-Class Mail. Further, USPS's total unfunded liabilities and debt were $143 billion at the end of fiscal year 2018, an amount double its annual revenue.

As we testified in February 2017, a comprehensive package of legislative actions is needed to improve USPS's financial viability. In that testimony, we also stated that USPS's financial situation leaves Congress with difficult choices and trade-offs to achieve the broad-based restructuring that will be necessary for USPS to become financially sustainable.

In addition, USPS has missed $48.2 billion in required payments for postal retiree health and pension benefits through fiscal year 2018, including $42.6 billion in missed payments for retiree health benefits since fiscal year 2010, and $5.6 billion for pension benefits since fiscal year 2014. USPS has stated that it missed these payments to minimize the risk of running out of cash, citing its precarious financial condition and the need to cover current and anticipated costs and any contingencies.

USPS appears likely to miss required payments for retiree health benefits for the foreseeable future. Based on Office of Personnel Management projections, the fund supporting postal retiree health benefits would be depleted in fiscal year 2030 if USPS continues to miss all payments. If the fund is depleted, USPS would be required by law to make the payments necessary to cover its share of health benefits premiums for postal retirees. However, current law does not address what would happen if USPS misses those payments. Depletion of the fund, together with USPS's potential inability to make remaining contributions, could affect postal retirees as well as USPS, customers, and other stakeholders, including the federal government.

## What Remains to Be Done

As USPS has stated, it needs to aggressively pursue additional cost-reduction initiatives in areas in which it has managerial discretion. Because USPS actions under its existing authority will be insufficient to restore its financial viability, a balanced package of legislative reform continues to be needed.

### Congressional Actions Needed

Congress should consider a comprehensive package of legislative actions to improve USPS's financial viability, including (1) facilitating USPS's ability to better align costs with revenues; (2) putting postal retiree health benefits on a more sustainable financial footing; and (3) requiring any binding arbitration in the negotiation process for USPS labor contracts to take USPS's financial condition into account. Congress should consider various options to better align USPS costs with revenues, and address constraints and legal restrictions that limit USPS's ability to reduce costs and improve efficiency.

## Related GAO Products

*Postal Retiree Health Benefits: Unsustainable Finances Need to Be Addressed*. GAO-18-602. Washington, D.C: August 31, 2018.

*U.S. Postal Service: Projected Capital Spending and Processes for Addressing Uncertainties and Risks*. GAO-18-515. Washington, D.C.: June 28, 2018.

*International Mail: Information on Changes and Alternatives to the Terminal Dues System*. GAO-18-112. Washington, D.C.: October 12, 2017.

*U.S. Postal Service: Key Considerations for Potential Changes to USPS's Monopolies*. GAO-17-543. Washington, D.C.: June 22, 2017.

*U.S. Postal Service: Key Considerations for Restoring Fiscal Sustainability*. GAO-17-404T. Washington, D.C.: February 7, 2017.

*U.S. Postal Service: Continuing Financial Challenges and the Need for Postal Reform*. GAO-16-651T. Washington, D.C.: May 11, 2016.

*U.S. Postal Service: Financial Challenges Continue*. GAO-16-268T. Washington, D.C.: January 21, 2016.

# Improving the Management of IT Acquisitions and Operations

To better manage billions of dollars in information technology (IT) investments, the Office of Management and Budget (OMB) and other federal agencies should further implement the requirements of federal IT acquisition reforms.

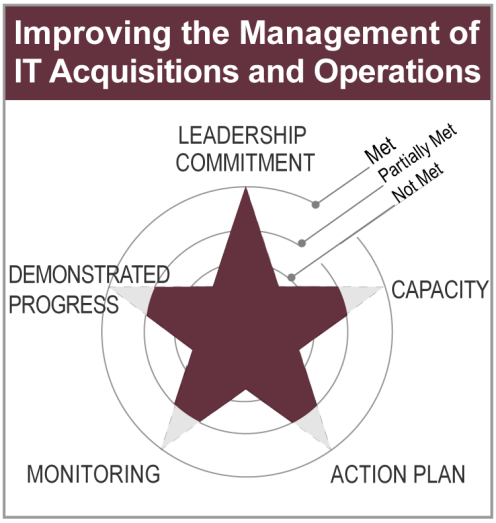
**Why Area Is High Risk**

The executive branch has undertaken numerous initiatives to better manage the more than $90 billion that is annually invested in IT. However, federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. These investments often suffered from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance. In 2015, we added the government's management of IT acquisitions and operations to the High-Risk list.

Recognizing the severity of issues related to the government-wide management of IT, in December 2014, Congress and the President enacted federal IT acquisition reform legislation; in November 2017, the sunset dates of several of these statutory provisions were extended or removed. Among other things, these laws require covered agencies to: (1) enhance agency CIO authority, (2) enhance transparency and improve risk management, (3) consolidate federal data centers, (4) review IT investment portfolios, (5) purchase government-wide software licenses, (6) maximize the benefit of federal strategic sourcing and (7) expand training and use of IT acquisition cadres.

**Contact Information**

For additional information about this high-risk area, contact Carol Harris at 202-512-4456 or harriscc@gao.gov.




Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, ratings for all five criteria remain unchanged.

**Leadership commitment: met.** OMB continues to demonstrate its leadership commitment by (1) issuing guidance for covered departments and agencies (agencies) to implement statutory provisions commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA), (2) optimizing federal data centers, and (3) acquiring and managing software licenses. It will be important for OMB to maintain its current level of top leadership support and commitment to ensure that agencies successfully execute OMB's guidance on implementing FITARA and related IT initiatives. Sustained Congressional focus on implementing FITARA has led to improvement, as highlighted in agencies' FITARA implementation scores issued biannually by the House Committee on Oversight and Reform. However, further Executive branch and Congressional attention is required.

**Capacity: partially met.** OMB has established guidance for FITARA and related IT management practices that addresses how agencies are to implement roles and responsibilities. The guidance covers, among other things, enhancing the authority of federal chief information officers (CIO) and ensuring that program staff has the necessary knowledge and skills to effectively acquire IT. As we reported in August 2018, none of the 24 major federal agencies had IT management policies that fully addressed the role of their CIOs consistent with federal laws and guidance. The majority of the agencies minimally addressed or did not address their CIO's role in assessing agency IT workforce needs, and developing strategies and plans for meeting those needs. Correspondingly, the majority of the 24 CIOs acknowledged they were not fully effective at implementing IT workforce responsibilities.

In November 2016, we reported that while the five agencies we reviewed had demonstrated important progress in implementing key IT workforce planning activities, each had shortfalls. For example, four agencies had

not demonstrated an established IT workforce planning process. All five agencies either agreed or partially agreed with our recommendations and identified planned actions to address our recommendations to improve their IT workforce planning. However, as of December 2018, none of our recommendations had been fully implemented.

**Action plan: partially met.** In addition to requiring covered agencies to conduct self-assessments, OMB's FITARA implementation guidance requires agencies to develop and implement plans describing changes they will make to ensure that IT management responsibilities for CIOs and other senior agency officials are effectively implemented. These plans are to address the areas of IT management that we have identified as high risk, such as reviewing poorly performing investments, managing agencies' IT portfolios, and implementing incremental development. While all 24 major federal agencies have developed FITARA implementation plans, the agencies need to demonstrate additional progress in effectively implementing these plans. As of December 2018, our continuing work to monitor progress in this area showed that 22 of the 24 major federal agencies had publicly reported at least partial completion of their FITARA milestones; however, all 22 of those agencies also reported incomplete milestones.

Significant work remains for federal agencies to establish action plans to modernize or replace obsolete IT investments. In May 2016, we reported that agencies were using systems which had components that were, in some cases, at least 50 years old. To address this issue, we recommended that 12 agencies identify and plan to modernize or replace legacy systems, including establishing time frames, activities to be performed, and system functions to be replaced or enhanced. Of the 12 agencies, 10 either concurred or partially concurred with our recommendations, while 2 stated they had no comment. However, as of December 2018, only 3 of the 12 agencies had implemented our recommendation and made progress in planning to modernize their legacy systems.

**Monitoring: partially met.** The President's Management Agenda identified improving IT spending transparency as one of the Administration's 14 cross-agency priority goals and tasked OMB with leading the drive towards better agency reporting on IT spending.

In January 2018, we reported that the majority of 22 agencies that we reviewed did not identify all of their IT contracts, leaving about $4.5 billion in IT-related contract obligations beyond those reported by agencies. Further, in November 2018, we reported that four selected agencies lacked quality assurance processes for ensuring that billions of dollars requested in their IT budgets were informed by reliable cost information. We made recommendations for those agencies to improve how IT acquisitions are identified and to establish procedures for ensuring IT budgets are informed by reliable cost information. Until agencies properly

identify IT acquisitions and establish processes for ensuring the quality of cost data used to inform their IT budgets, agency CIOs are at risk of not having appropriate oversight of IT acquisitions worth billions of dollars and not having adequate transparency into IT spending to make informed budget decisions.

OMB has taken action to improve monitoring through its IT Dashboard—a public website that provides detailed information on major IT investments at 26 federal agencies, including ratings from CIOs that should reflect the level of risk facing each investment. However, in June 2016, we reported that our assessments of IT Dashboard risk ratings showed more risk on the majority of agency IT investments we sampled than did the associated CIO ratings. Consequently, we made 25 recommendations to 15 agencies to improve their CIO's risk ratings; 12 agencies generally agreed with or did not comment on our recommendations, and 3 disagreed. As of December 2018, only 14 of the recommendations had been fully implemented. Agencies should continue to fully and accurately report on these risks to ensure their IT investments receive appropriate oversight.

An additional area of concern regarding the monitoring of IT acquisitions is agencies' reported use of incremental development; OMB policy requires that IT investments deliver functionality in 6-month increments. However, our May 2014 report found that delivery rate to be challenging for agencies and, thus, we recommended that OMB instead require increments of 12 months. While OMB disagreed with our recommendation, our continuing work in this area has found that most agencies have reported progress in improving the rate at which their IT acquisitions deliver functionality at the 12-month rate. Nonetheless, in November 2017, we reported that most agencies lacked the required policies intended to ensure adequate consideration of incremental development approaches for major IT investments and we made 19 recommendations to 17 agencies to address this issue. Eleven agencies agreed with our recommendations, 1 partially agreed, and 5 did not state whether they agreed or disagreed. As of December 2018, 11 of our 19 recommendations remained open.

**Demonstrated progress: partially met.** In our 2017 high-risk update, we identified agency plans to save $5.3 billion from data center consolidation, a number which included $3.3 billion planned through fiscal year 2015. Agencies subsequently reported achieving $2.8 billion of that amount. In 2016, OMB issued new guidance on consolidating data centers and subsequently, a number of agencies revised their planned savings, resulting in $2.4 billion planned from fiscal years 2016 through 2018. As of August 2018, our continuing work to monitor progress in this area has shown that over $1.9 billion of that savings had been achieved. The total achieved savings of $4.7 billion represents slightly more than 80 percent of the agencies' planned $5.7 billion in savings since 2011. In our 2017 high-risk update, we cited this 80 percent target as one of several actions

that should be taken and recognize the positive government-wide progress this demonstrates. However, improvement is still needed in other areas.

Since fiscal year 2010, we have made 1,242 recommendations to address shortcomings in IT acquisitions and operations; 514 since this area was added to the High-Risk List in February 2015. As of December 2018, OMB and federal agencies had fully implemented only 735 (or about 59 percent) of the total recommendations and only 169 (about 33 percent) of the recommendations made since February 2015. In addition, agencies have made progress in achieving about $2.5 billion in savings across a key OMB initiative—PortfolioStat—intended to improve the management of IT investments by consolidating and eliminating duplicative systems, among other things. Through fiscal year 2016, agencies had saved almost $1.8 billion, with more than $754 million in fiscal year 2017. Nevertheless, agencies have approximately $3.5 billion in their reported planned savings still to be achieved.

## What Remains to Be Done

As we have recommended, OMB and covered federal agencies should further implement the requirements of FITARA. OMB will need to provide sustained oversight to ensure that agency actions are completed and the desired results are achieved.

- Beyond implementing FITARA and OMB's guidance to improve the capacity to address our high-risk area, agencies need to implement our recent recommendations related to improving CIO authorities, as well as past recommendations on improving IT workforce planning practices.
- Agencies must establish action plans to modernize or replace obsolete IT investments.
- Agencies need to implement our recommendations to address weaknesses in their IT Dashboard reporting of investment risk and incremental development implementation.
- OMB and agencies should work toward implementing our remaining 456 open recommendations related to this high-risk area. These remaining recommendations include 12 priority recommendations for agencies to, among other things, report all data center consolidation cost savings to OMB, plan to modernize or replace obsolete systems as needed, and improve their implementation of PortfolioStat. OMB and agencies need to take additional actions to (1) implement at least 80 percent of our open recommendations related to the management of IT acquisitions and operations, (2) ensure that a minimum of 80 percent of the government's major IT acquisitions deliver functionality every 12 months, and (3) achieve at least 80 percent of the over $6 billion in planned PortfolioStat savings.

## Related GAO Products

*Information Technology: Departments Need to Improve Chief Information Officers' Review and Approval of IT Budgets*. GAO-19-49. Washington, D.C.: November 13, 2018.

*Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*. GAO-18-93. Washington, D.C.: August 2, 2018.

*Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*. GAO-18-264. Washington, D.C.: May 23, 2018.

*Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions*. GAO-18-42. Washington, D.C.: January 10, 2018.

*Information Technology: OMB Needs to Report On and Improve Its Oversight of the Highest Priority Programs*. GAO-18-51. Washington, D.C.: November 21, 2017.

*Information Technology Reform: Agencies Need to Improve Certification of Incremental Development*. GAO-18-148. Washington, D.C.: November 7, 2017.

*Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal*. GAO-17-448. Washington, D.C.: August 15, 2017.

*Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*. GAO-17-388. Washington, D.C.: May 18, 2017.

*Information Technology: Opportunities for Improving Acquisitions and Operations*. GAO-17-251SP. Washington, D.C.: April 11, 2017.

# 2020 Decennial Census

For the 2020 Census, the U.S. Census Bureau (Bureau) plans to implement several innovations, including new IT systems. The challenges associated with successfully implementing these innovations, along with other challenges, puts the Bureau's ability to conduct a cost-effective census at risk.

**Why Area Is High Risk**

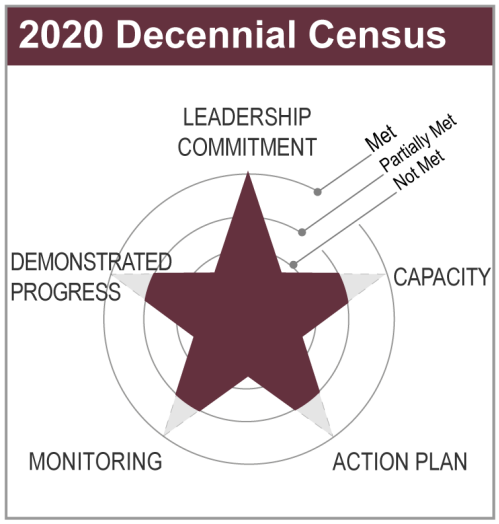
The U.S. Census is mandated by the Constitution and provides vital data for the nation. Census data are used, among other purposes, to apportion the seats of the U.S. House of Representatives; redraw congressional districts in each state; and allocate billions of dollars each year in federal financial assistance. Further, businesses use census data to market new services and products, and to tailor existing ones to demographic changes.

The Bureau is seeking to control the cost of the census, which has been escalating with each decade. The 2020 Census is now estimated to cost approximately $15.6 billion. Moreover, the average cost for counting a housing unit increased from about $16 in 1970 to around $92 in 2010 (in 2020 constant dollars), in part because the nation's population is more difficult to count.

The Bureau is also implementing several new innovations that require managing the processes of acquiring and developing new and modified IT systems. In addition, because the 2020 Census involves collecting personal information from over a hundred million households, it will be important that the Bureau addresses system security weaknesses in a timely manner, and that risks are at an acceptable level before systems are deployed.

**Contact Information**

For additional information about this high-risk area, contact Robert Goldenkoff at 202-512-2757 or goldenkoffr@gao.gov, or Nick Marinos at 202-512-9342 or marinosn@gao.gov.




Source: GAO analysis. | GAO-19-157SP

The 2020 Decennial Census was first added in 2017 as a high-risk area. Since then, the Bureau has met the criterion for leadership commitment and made progress on the other four criteria.

**Leadership commitment: met.** The Bureau and the Department of Commerce have strengthened this area with executive-level oversight of the 2020 Census by holding regular meetings on the status of IT systems and other risk areas. In addition, in 2017 the Department of Commerce designated a team to assist senior Bureau management with cost estimation challenges. Moreover, on January 2, 2019, a new Director of the Census Bureau took office, a position that had been vacant since June 2017; and in June 2018 the once-vacant Deputy Director position was filled.

**Capacity: partially met.** To enhance the capacity of its Decennial Directorate, the Bureau brought in new leadership in October 2017 with significant experience in program execution. The Bureau also improved the cost estimation process of the decennial when it established guidance including:

- roles and responsibilities for oversight and approval of cost estimation processes,
- procedures requiring a detailed description of the steps taken to produce a high-quality cost estimate, and
- a process for updating the cost estimate and associated documents over the life of a project.

However, the Bureau continues to experience skills gaps in the government program management office overseeing the $886 million contract for integrating the IT systems needed to conduct the 2020 Census. Specifically, as of November 2018, 21 of 44 positions in this office were vacant. These vacant positions add risk that the office may not be able to provide adequate oversight of contractor cost, schedule, and performance.

**Action plan: partially met.** In December 2018, the Bureau issued an updated operational plan for the 2020 Census that laid out risks, decisions made, issues to be resolved, and related milestones for each of its major operations. However, the 2020 Census schedule lacks a risk assessment and certain other best scheduling practices, which affects its overall reliability. In addition, during the 2018 End-to-End Test we found the Bureau's data management reporting system did not always provide accurate information because of a software issue. As a result, Bureau staff had to rely on multiple systems to manage field operations, making monitoring inefficient.

**Monitoring: partially met.** The Department of Commerce holds biweekly meetings with Bureau leadership to discuss the status of 2020 Census operations, including our open recommendations. To track performance of decennial census operations, the Bureau relied on reports to track progress against pre-set goals for a test conducted in 2018. According to the Bureau, these same reports will be used in 2020 to track progress.

The Bureau has also taken steps to improve its cost estimation process for 2020; however, it needs to implement a system to track and report variances between actual and expected cost elements. Further, the Bureau's schedule for developing IT systems during the 2018 End-to-End Test experienced delays that compressed the time available for system testing, integration testing, and security assessments. These schedule delays contributed to systems experiencing problems after deployment, as well as cybersecurity challenges. For example, as of December 2018, the Bureau had identified nearly 1,100 system security weaknesses that needed to be addressed.

**Demonstrated progress: partially met.** According to Department of Commerce officials, in the summer of 2018, the Bureau began conducting an analysis of oversight recommendations, including ours, to determine the root cause of shortfalls and set a timeline for addressing those recommendations and related root causes. We have standing quarterly meetings with Senior Bureau officials to discuss the status and expected actions for our open recommendations related to the 2020 Census. We also periodically meet with the Under Secretary for Economic Affairs to discuss the Department of Commerce's oversight of the decennial census.

The Bureau is also using the cost estimate as a management tool for making decisions and assessing tradeoffs. For example, the cost estimate served as the basis for the fiscal year 2019 funding request developed by the Bureau. The Bureau also said it used the 2020 Census cost estimate to establish cost controls during budget formulation activities and to monitor spending levels for fiscal year 2019 activities.

While these actions and others are important steps forward, we found that the Bureau scaled back testing of new innovations in 2017 and 2018.

Specifically, the Bureau cancelled the field portion of the 2017 test and then conducted a full operational test in only one site—Providence County, Rhode Island—instead of three test sites as originally planned. Moreover, the Bureau did not test all 2020 Census systems and IT capabilities during its operational test. Not fully testing innovations and IT systems as designed, increases the risk that innovations and IT systems will not function as intended during the 2020 Census.

## What Remains to Be Done

As of January 2019, we have made 97 recommendations related to the 2020 Census. The Bureau has implemented 67 of these recommendations and 30 remain open. The Department of Commerce generally agreed with our recommendations and is taking steps to implement them. Moreover, in our April 2018 priority recommendation letter to the Department of Commerce we identified 15 recommendations as priority—seven of which have been closed as implemented over the past year. To make continued progress, the Bureau needs to ensure its approach to strategic planning, IT management, cybersecurity, human capital management, internal collaboration, knowledge sharing, as well as risk and change management are aligned toward delivering more cost-effective outcomes. Specifically the Bureau needs to:

- fill vacant positions in its government program management office as needed to oversee the IT integration contractor;
- implement best practices for scheduling the thousands of activities that make up the 2020 Census;
- improve the management and oversight of its IT systems in order to meet milestones for system development and testing, and be ready for the major operations of the 2020 Census;
- address cybersecurity weaknesses in a timely manner and ensure that risks are at an acceptable level before systems are deployed;
- implement cost estimation best practices including a system to track and report variances between actual and expected costs for its 2020 Census cost estimate;
- resolve implementation issues that have arisen during testing, prior to the 2020 Census; and
- continue to address our recommendations, especially those designated priority recommendations.

## Congressional Actions Needed

In 2017 and 2018, we testified in five congressional hearings focused on the progress of the Bureau's preparations for the decennial census. Going forward, continued congressional oversight will be needed to ensure decennial efforts stay on track, the Bureau has needed resources, and Bureau officials are held accountable for implementing the enumeration as planned.

## Related GAO Products

*2020 Census: Additional Steps Needed to Finalize Readiness for Peak Field Operations*, GAO-19-140. Washington, D.C.: December 10, 2018.

*2020 Census: Continued Management Attention Needed to Address Challenges and Risks with Developing, Testing, and Securing IT Systems*, GAO-18-655. Washington, D.C.: August 30, 2018.

*2020 Census: Census Bureau Improved the Quality of Its Cost Estimation but Additional Steps Are Needed to Ensure Reliability*, GAO-18-635. Washington, D.C.: August 17, 2018.

*2020 Census: Bureau Has Made Progress with Its Scheduling, but Further Improvement Will Help Inform Management Decisions*, GAO-18-589. Washington, D.C.: July 26, 2018.

*2020 Census: Actions Needed to Address Challenges to Enumerating Hard-to-Count Groups*, GAO-18-599. Washington, D.C.: July 26, 2018.

*2020 Census: Actions Needed to Improve In-Field Address Canvassing Operation*, GAO-18-414. Washington, D.C.: June 14, 2018.

*2020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration*, GAO-18-543T. Washington, D.C.: May 8, 2018.

*2020 Census: Continued Management Attention Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration*, GAO-18-416T. Washington, D.C.: April 18, 2018.

*2020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective Enumeration*, GAO-18-215T. Washington, D.C.: October 31, 2017.

*2020 Census: Continued Management Attention Needed to Oversee Innovations, Develop and Secure IT Systems, and Improve Cost Estimation*, GAO-18-141T. Washington, D.C.: October 12, 2017.

*2020 Census: Bureau Is Taking Steps to Address Limitations of Administrative Records*, GAO-17-664. Washington, D.C.: July 26, 2017.

# Government-wide Personnel Security Clearance Process

The government-wide personnel security clearance process continues to face challenges in the timely processing of clearances, measuring the quality of investigations, and ensuring the security of related information technology (IT) systems.

**Why Area Is High Risk**

We placed the government-wide personnel security clearance process on the High-Risk List in January 2018 because it faces significant challenges related to (1) the timely processing of clearances, (2) measuring investigation quality, and (3) ensuring IT security, among other things.

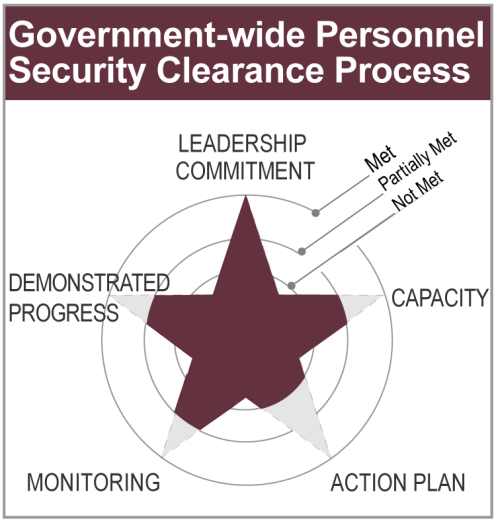
**Timeliness.** The executive branch has been unable to process personnel security clearances within established timeliness objectives, contributing to a backlog that the NBIB reported to be approximately 565,000 cases as of February 2019.

**Quality.** A high-quality personnel security clearance process minimizes the risks of unauthorized disclosures of classified information and helps ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed. While the executive branch has taken some steps to address quality, it has not established measures to ensure the quality of background investigations and adjudications, and instead focused on reducing the backlog and redesigning the investigation process.

**IT Security.** DOD is building and managing the development of the NBIS, but security concerns posed by DOD regarding OPM legacy IT systems may delay planned milestones for the new system. OPM did not effectively monitor actions taken to remediate identified weaknesses in its IT systems to ensure that key security controls are in place and operating as intended.

**Contact Information**

For additional information about this high-risk area, contact Brenda S. Farrell, 202-512-3604, or farrellb@gao.gov.




Source: GAO analysis. | GAO-19-157SP

Since we added the government-wide personnel security clearance process to our High-Risk List in January 2018, the executive branch has taken some action and made some progress addressing our criteria for removal. The executive branch has met the criterion for leadership commitment, partially met the capacity, monitoring, and demonstrated progress criteria, and has not met the action plan criterion. In addition, the administration proposed transferring the background investigation function from the Office of Personnel Management's (OPM) National Background Investigations Bureau (NBIB) to the Department of Defense (DOD) in June 2018, and plans to issue an Executive Order regarding the transfer.

**Leadership commitment: met.** The Security Clearance, Suitability, and Credentialing Performance Accountability Council (PAC), chaired by the Deputy Director for Management of the Office of Management and Budget (OMB), is the government-wide entity responsible for driving the implementation of and overseeing security clearance reform, among other reform efforts. The chair of the PAC, who is concurrently serving as the Acting Director of OPM, stated that the security clearance reform process is one of her top three government-wide priorities. Further, according to officials, the PAC assembled teams of stakeholders who meet regularly to focus on developing solutions to specific problems within the security clearance process. OPM and the Office of the Director of National Intelligence (ODNI) also issued a memo in June 2018 containing measures to reduce the backlog of background investigations. While the PAC has prioritized the prompt reduction of the backlog, it has not finalized a plan to reduce it to a manageable level or prioritized improving the timeliness of investigations.

Senior DOD officials expressed commitment to the administration's June 2018 transfer proposal and have planning efforts underway related to the transfer and the modernization of the personnel vetting process. Continued and coordinated leadership by the PAC will be important as it

works to complete other long-standing key reform initiatives, including the government-wide implementation of continuous evaluation. Focused leadership will also be critical throughout the transition of background investigative functions from OPM to DOD, as proposed by the administration, particularly during senior leadership changes at OPM and DOD.

**Capacity: partially met.** NBIB officials reported that NBIB has increased its workforce to approximately 8,700 federal and contract investigators to help address the investigations backlog. However, NBIB has not reported goals for increasing total investigator capacity or completed the development and implementation of a comprehensive strategic workforce plan, as we have recommended. Completing the workforce plan would better position the bureau to meet current and future demands for its services.

In addition, in August 2017, DOD submitted to the congressional defense committees a plan for the transfer of certain DOD background investigations from OPM's NBIB to DOD. This plan included estimates of the number of full-time equivalent employees necessary to execute the transfer. However, officials told us in November 2018 that the department is no longer using the plan because it was overcome by the administration's June 2018 organizational reform proposal for the complete transfer of the NBIB background investigation program from OPM to DOD. According to officials, DOD is now preparing for the transfer of all NBIB investigative functions by developing a new plan which is based on the total inventory of OPM's background investigations. In preparation for the transfer, DOD should consider our recommendation to the Director of NBIB to develop a strategic workforce plan as it assumes these responsibilities.

Executive Order 13467, as amended, which establishes the PAC, among other things, assigns the Secretary of Defense the role of developing and securely operating IT systems that support all background investigation processes conducted by NBIB (Exec. Order No. 13467, § 2.6(b), as amended through Exec. Order No. 13764, 82 Fed. Reg. 8115, 8126 (Jan. 17, 2017). In addition, the National Defense Authorization Act (NDAA) for Fiscal Year 2018 included a provision that DOD conduct a review of the National Background Investigation Services (NBIS), the IT system it is developing to support background investigations, to determine whether certain enhancements are necessary (see Pub. L. No. 115-91, § 925(f) (2017)). According to officials, DOD has in place the resources needed for the development of NBIS, is actively identifying necessary system capabilities, and has begun small preliminary pilots of its services. However, according to officials, the necessary resources for full implementation of NBIS and the administration's transfer proposal remain unclear.

**Action plan: not met.** The leaders of the reform effort have developed various plans for more than a decade to improve the process. Most recently, in March 2018, the Director of National Intelligence (DNI) issued implementation guidelines for continuous evaluation—a process to review the background of clearance holders and individuals in sensitive positions at any time during the eligibility period. Further, DOD has begun reorganizing certain entities within the department that will enable DOD to begin the transfer of investigative functions from OPM's NBIB. While the DNI and OPM have issued a joint Executive Correspondence that contains measures clarifying and adjusting certain elements of investigation requirements, the PAC lacks plans, including goals and milestones, to (1) reduce the backlog to a manageable level; (2) meet timeliness objectives for security clearance investigations and adjudications; and (3) assess and address the potential effects of continuous evaluation on agency resources.

Officials from ODNI, DOD, and the PAC told us they are working on an initiative called Trusted Workforce 2.0, an effort to transform the fundamental approach to workforce vetting, and supporting policies that will also overhaul business processes and modernize the IT architecture. According to officials, this effort is an expansion of reform since our January 2018 high-risk designation that will consider both risk and trust. PAC and ODNI officials said Trusted Workforce 2.0 will focus on timeliness and quality goals in a future phase, after reducing the clearance backlog to a manageable level. The DNI and former Director of OPM committed to issuing this new policy framework and plans to transform vetting for the Executive Branch by the end of 2018. Officials told us in early 2019 that the issuance of related policies is expected throughout the calendar year.

**Monitoring: partially met.** The NDAA for Fiscal Year 2018 required the DNI, in coordination with the other PAC principals, to annually report for the prior fiscal year on the timeliness of initiations, investigations, and adjudications, by clearance level. This report is to cover both initial investigations and periodic reinvestigations for government and contractor employees (see Pub. L. No. 115-91, § 925(k)(1)). In November 2018, the DNI informed executive branch agencies that it intends to fulfill this and other legislative reporting requirements through a consolidated data call.

In September 2018, NBIB reported to Congress, for each clearance level, (1) the size of the investigation backlog, (2) the average length of time to conduct an initial investigation and a periodic reinvestigation, and (3) a discussion of the factors contributing to investigation timeliness. The PAC is also reporting publicly on the progress of key reforms through www.performance.gov, where OMB began tracking security clearance and suitability reform as a cross-agency priority goal in March 2014. For fiscal year 2018, www.performance.gov contains quarterly action plans and progress updates, which present figures on the average timeliness of

initial investigations and periodic reinvestigations for the executive branch as a whole, investigation workload and backlog, and investigator headcounts.

Our analysis of the latest available timeliness data showed that the number of executive branch agencies meeting investigative and adjudicative objectives decreased from fiscal years 2012 through 2018. Furthermore, the PAC has not implemented our December 2017 recommendation to conduct an evidence-based review of the investigation and adjudication timeliness objectives for completing the fastest 90 percent of initial secret and initial top secret security clearances. In addition, the PAC has not yet established performance measures to monitor investigation and adjudication quality, continuous evaluation implementation, and government-wide reciprocity.

**Demonstrated progress: partially met.** The PAC has demonstrated progress in some areas, specifically related to a reduction in the backlog of background investigations. NBIB officials report that the backlog decreased from almost 715,000 cases in January 2018—when we added the process to our High-Risk List—to approximately 565,000 cases in February 2019. Those officials credit an Executive Memorandum—issued jointly in June 2018 by the DNI and the Director of OPM and containing measures to reduce the investigation backlog—as a driver in backlog reduction. The measures adjust investigative requirements by, for example, temporarily allowing for video or telephone interviews in certain circumstances. We will continue to monitor the backlog and efforts to reduce it.

While members of the PAC have taken positive steps to improve continuous evaluation and reciprocity, including the DNI's March 2018 continuous evaluation implementation guidelines and November 2018 guidance providing requirements for reciprocity, the PAC has not demonstrated sustained progress to address other weaknesses we have identified. For example, PAC leaders have not completed the development of quality measures for investigations, and PAC officials told us they had not made plans to report quality to Congress.

Further, the PAC has not demonstrated measurable improvements with regards to the timeliness of background investigations and adjudications. In fiscal year 2018, the percent of agencies meeting the timeliness objectives in which the fastest 90 percent are to be completed within a specified number of days are presented in table 6 below.

**Table 6: Percent of Executive Branch Agencies Meeting Security Clearance Processing Timeliness Objectives in Fiscal Year 2018**

| Phase | Type | Objective | Percentage Meeting Objective |
|---|---|---|---|
| Investigation | Initial Secret | 40 days | 3 percent |
| | Initial Top Secret | 80 days | 13 percent |
| | Periodic reinvestigations | 150 days | 13 percent |
| Adjudication | Initial Secret | 20 days | 44 percent |
| | Initial Top Secret | 20 days | 44 percent |
| | Periodic reinvestigations | 30 days | 65 percent |

Source: GAO analysis of Office of the Director of National Intelligence data. | GAO-19-157SP

Agencies without delegated authority rely on OPM to conduct their background investigations, while agencies with delegated authority have been authorized to conduct their own background investigations. As such, investigative phase timeliness data for agencies without delegated authority is generally a reflection of OPM's timeliness. While the data ODNI provided shows that timeliness continues to decline, OPM officials stated that NBIB internal monitoring shows recent improvement in investigation timeliness.

## What Remains to Be Done

We have made numerous recommendations to PAC members to address risks associated with the personnel security clearance process between 2011, when we removed DOD's personnel security clearance program from the High-Risk List and 2018, when we placed the government-wide personnel security clearance process on the High-Risk List. We consider 27 of those recommendations key to addressing the high-risk designation. Eight recommendations key to the high-risk designation have been implemented, including three since January 2018. Most recently, those recommendations implemented include ODNI formalizing plans and guidance for continuous evaluation. As of December 2018, 19 of these key recommendations remain open. Of the open recommendations, ODNI stated that it did not concur with our December 2017 recommendations on addressing investigation quality and timeliness, but did not provide specific information to explain why it did not concur.

In addition, in March 2018, we outlined necessary actions and outcomes—anchored in each of our five criteria for removal from the High-Risk List—and our prior recommendations that need to be addressed for this area to be removed. These actions and outcomes are outlined below and should be considered by all four agencies, unless a lead agency is indicated.

To continue to meet the leadership commitment criterion, these agencies should:

- continue to demonstrate that the PAC is prioritizing the (1) prompt reduction of the government-wide investigative backlog to a manageable level; (2) improvement of the timeliness of background investigations; and (3) completion of long-standing, key reform initiatives;
- continue participating regularly in leadership meetings of the PAC principals;
- provide the necessary oversight and support to PAC members to effectively accomplish assigned reform initiatives, in accordance with the roles and responsibilities outlined in Executive Order 13467 (as amended), as Chair of the PAC (OMB); and
- oversee and support NBIB and DOD during the transition period while DOD stands up background investigative functions, to include supporting resource needs.

To make progress on meeting capacity, these agencies should:

- develop and implement a comprehensive strategic workforce plan that identifies the workforce needed to meet the current and future demand for its services, as well as reduce the current backlog to a manageable level (OPM, DOD);
- coordinate with responsible executive branch agencies to identify the resources needed to effectively implement personnel security clearance reform effort initiatives within established timeframes (OMB, ODNI, DOD); and
- develop long-term funding estimates for changes to the federal government's investigation practices resulting from the implementation of the 2012 Federal Investigative Standards. These long-term funding estimates should include, but not be limited to: (1) costs related to IT adjustments to enable government-wide data sharing; (2) costs related to implementing continuous evaluation; and (3) costs related to the changed frequency of periodic reinvestigations (OMB).

To make progress on an action plan, these agencies should:

- develop a plan, including goals and milestones, for reducing the backlog of background investigations to a manageable level;
- develop a government-wide plan, including goals and interim milestones, to meet timeliness objectives for initial personnel security clearances, periodic reinvestigations, and adjudications; and
- assess the potential effects of continuous evaluation on agency resources and develop a plan to address those effects, such as modifying the scope of periodic reinvestigations, changing the frequency of periodic reinvestigations, or replacing periodic reinvestigations for certain clearance holders (ODNI).

To make progress on monitoring, these agencies should:

- develop and report to Congress annually on government-wide, results-oriented performance measures for the quality of security clearance background investigations and adjudications (ODNI);
- develop performance measures for continuous evaluation that agencies must track and regularly report to ODNI;
- develop metrics and government-wide baseline data for reciprocity determinations to measure the extent of reciprocity within the executive branch and report on those metrics to Congress (ODNI); and
- monitor the implementation of remedial actions intended to resolve known cybersecurity vulnerabilities, to include updating remedial action plans to reflect expected completion dates, and improve the timeliness of validating the effectiveness of actions taken to mitigate cybersecurity vulnerabilities that exposed agency information to cybersecurity incidents (OPM).

To improve on demonstrating progress, these agencies should:

- develop government-wide performance measures for the quality of background investigations and adjudications (OMB, ODNI);
- conduct an evidence-based review of the investigation and adjudication timeliness objectives for completing the fastest 90 percent of initial secret and initial top secret security clearances, and take action to adjust the objectives if appropriate;
- conduct an evidence-based review of the timeliness goal of 195 days for completing the fastest 90 percent of periodic reinvestigations and the associated goals for the different phases of periodic reinvestigations, and adjust the goal if appropriate; and
- improve and secure personnel security clearance IT systems, including implementing further security improvements to its IT environment, including contractor-operated systems, to ensure that key security controls are in place and operating as intended (OPM).

## Congressional Actions Needed

The annual assessments of timeliness and quarterly briefings required by the NDAA for Fiscal Year 2018 will serve as mechanisms for Congress and the executive branch to monitor timeliness, costs, and continuous evaluation, among other things.

## Related GAO Products

*Personnel Security Clearances: Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations*. GAO-18-431T. Washington, D.C.: March 7, 2018.

*Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timeliness, and Reduce Investigation Backlog*. GAO-18-29. Washington, D.C.: December 12, 2017.

*Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders*. GAO-18-117. Washington, D.C.: November 21, 2017.

*Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*. GAO-17-614. Washington, D.C: August 3, 2017.

*Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*. GAO-16-501. Washington, D.C.: May 18, 2016.

*Personnel Security Clearances: Funding Estimates and Government-wide Metrics Are Needed to Implement Long-Standing Reform Efforts*. GAO-15-179SU. Washington, D.C.: April 23, 2015.

# Ensuring the Cybersecurity of the Nation

Federal agencies and other entities need to take urgent actions to implement a comprehensive cybersecurity strategy, perform effective oversight, secure federal systems, and protect cyber critical infrastructure, privacy, and sensitive data.

**Why Area Is High Risk**

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being.

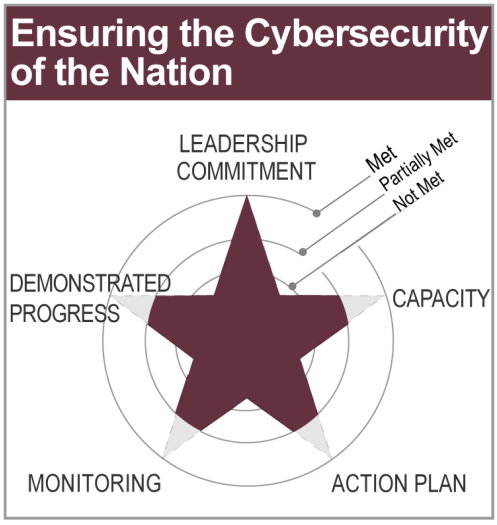
Because many of these systems contain vast amounts of personally identifiable information (PII), agencies must protect the confidentiality, integrity, and availability of this information. In addition, they must effectively respond to data breaches and security incidents when they occur.

The risks to IT systems supporting the federal government and the nation's critical infrastructure 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.

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 PII.

**Contact Information:**

For additional information about this high-risk area, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Vijay D'Souza at (202) 512-6240 or dsouzav@gao.gov.




Source: GAO analysis. | GAO-19-157SP

Since our previous 2017 High-Risk Report, our assessment of efforts to address all five criteria remains unchanged.

**Leadership commitment: met.** In May 2017, the President issued an executive order requiring federal agencies to take a variety of actions, including better managing their cybersecurity risks and coordinating to meet reporting requirements related to cybersecurity of federal networks and critical infrastructure. Further, in December 2017, the President issued a National Security Strategy citing cybersecurity as a national priority and identifying needed actions, such as identifying and prioritizing risk and building defensible government networks.

The administration further described its planned approach to cybersecurity with the release of a National Cyber Strategy in September 2018. This national strategy outlines activities such as securing critical infrastructure, federal networks, and associated information, as well as developing the cybersecurity workforce. To lead the nation's cybersecurity response activities, in November 2018, the President signed the Cybersecurity and Infrastructure Security Agency Act of 2018 into law. Among other things, the law enables the Department of Homeland Security (DHS) to restructure the existing cybersecurity components within the National Protection and Programs Directorate to create a new cyber-focused agency.

**Capacity: partially met.** In June 2018, the administration issued a government-wide reform plan and reorganization recommendations that included, among other things, proposals for solving the federal cybersecurity workforce shortage. In particular, the plan notes the administration's intent to prioritize and accelerate ongoing efforts to reform the way that the federal government recruits, evaluates, selects, pays, and places cyber talent. The plan further states that, by the end of the first quarter of fiscal year 2019, all 24 major federal agencies, in coordination with DHS and the Office of Management and Budget (OMB), are to develop a critical list of vacancies across their organizations.

Nevertheless, the federal government continues to face challenges in ensuring that the nation's cybersecurity workforce has the appropriate skills. For example, we have previously reported that DHS and the Department of Defense had not fully addressed cybersecurity workforce management requirements set forth in federal laws. Further, as of June 2018, most of the 24 major federal agencies had not fully implemented all requirements associated with the Federal Cybersecurity Workforce Assessment Act of 2015. For example, three agencies had not conducted a baseline assessment to identify the extent to which their cybersecurity employees held professional certifications. As a result, these agencies may not be able to effectively gauge the competency of individuals who are charged with ensuring the confidentiality, integrity, and availability of federal information and information systems.

**Action plan: partially met.** In response to the May 2017 presidential executive order, DHS issued a cybersecurity strategy in May 2018 that articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks over the next 5 years. Further, OMB issued the Federal Cybersecurity Risk Assessment and Action Plan in August 2018. The assessment stated that OMB and DHS examined the capabilities of 96 civilian agencies across 76 cybersecurity metrics and found that 71 agencies had cybersecurity programs that were either at risk or at high risk. The assessment also stated that agencies were not equipped to determine how malicious actors seek to gain access to their information systems and data. The assessment identified core actions to address cybersecurity risks across the federal enterprise.

Additionally, the September 2018 National Cyber Strategy outlined the administration's approach to cybersecurity through a variety of priority actions, such as centralizing management and oversight of federal civilian cybersecurity. However, the strategy lacks key elements that we have previously reported can enhance the usefulness of a national strategy, including clearly defined roles and responsibilities, and information on the resources needed to carry out the goals and objectives. Although the strategy states that National Security Council staff are to coordinate with departments, agencies, and OMB to determine the resources needed to support the strategy's implementation, it is unclear what official maintains overall responsibility for coordinating these efforts, especially in light of the elimination of the White House Cybersecurity Coordinator position in May 2018.[1]

Going forward, it will be critical for the White House to clearly define the roles and responsibilities of key agencies and officials in order to foster

[1]The White House Cybersecurity Coordinator position was created in December 2009 to, among other things, coordinate interagency cybersecurity policies and strategies, and to develop a comprehensive national strategy to secure the nation's digital infrastructure.

effective coordination and hold agencies accountable for carrying out planned activities to address the cybersecurity challenges facing the nation. We have work underway examining federal roles and responsibilities for protecting the nation against cyber threats, including the implications of the decision to eliminate the cybersecurity coordinator position. We expect to report on the results of our work by the end of fiscal year 2019.

**Monitoring: partially met.** DHS has established the National Cybersecurity and Communications Integration Center (NCCIC), which functions as the 24/7 cyber monitoring, incident response, and management center for the federal civilian government. The United States Computer Emergency Readiness Team, one of several subcomponents of the NCCIC, is responsible for operating the National Cybersecurity Protection System. Operationally known as Einstein, this system is intended to provide DHS with situational awareness related to cybersecurity of entities across the federal government, through intrusion detection and prevention capabilities.

Nevertheless, DHS has continued to be challenged in measuring how the NCCIC is performing its functions in accordance with mandated implementing principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities; however, as of December 2018, it had not established measures or other procedures for ensuring the timeliness of these assessments, as we previously recommended.

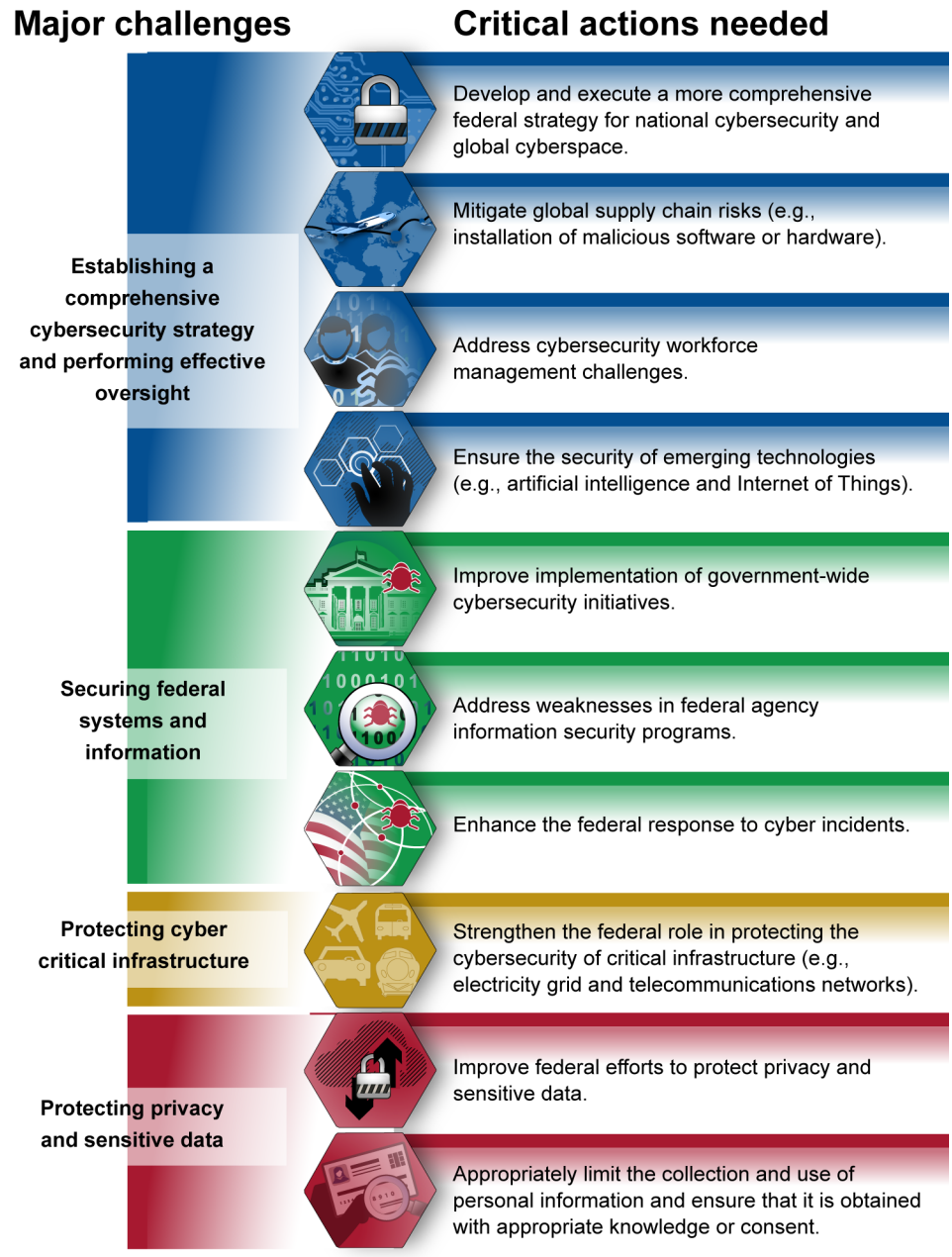
We also continued to find persistent weaknesses in federal agencies' monitoring of their information security programs. The Federal Information Security Modernization Act of 2014 (and its predecessor the Federal Information Security Management Act of 2002) requires federal agencies in the executive branch to develop, document, and implement an information security program and evaluate it for effectiveness. Our numerous security control audits have identified hundreds of deficiencies related to agencies' implementation of effective security controls.

**Demonstrated progress: partially met.** Since 2010, we have made over 3,000 recommendations to agencies aimed at addressing cybersecurity challenges facing the government—448 of which were made since the last high-risk update in February 2017. Nevertheless, many agencies face challenges in safeguarding their information systems and information, in part because many of these recommendations have not been fully implemented. Of the roughly 3,000 recommendations made since 2010, nearly 700 had not been fully implemented as of December 2018. We have also designated 35 as priority recommendations, meaning that we believe these recommendations warrant priority attention from heads of key departments and agencies. As of December 2018, 26 of our priority recommendations had not been fully implemented.

## What Remains to Be Done

Based on our prior work, we have identified four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address these challenges, we have identified 10 critical actions that the federal government and other entities need to take (see figure 5).

**Figure 5: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges**




Source: GAO analysis. | GAO-19-157SP

## Congressional Actions Needed

We also have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974 and the E-Government Act of 2002, because they may not consistently protect PII. Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government, and may not fully adhere to key privacy principles. However, the relevant revisions to the Privacy Act

and the E-Government Act had not yet been enacted as of the date of this report.

Further, we suggested that Congress consider strengthening the consumer privacy framework and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices. However, these suggested changes had not yet been enacted as of the date of this report.

## Related GAO Products

*Information Security: OPM Has Implemented Many of GAO's 80 Recommendations, but Over One-Third Remain Open*. GAO-19-143R. Washington, D.C.: November 13, 2018.

*Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*. GAO-18-518. Washington, D.C.: September 17, 2018.

*High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*. GAO-18-622. Washington, D.C.: September 6, 2018.

*Information Security: IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data*. GAO-18-391. Washington, D.C.: July 31, 2018.

*Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. GAO-18-559. Washington, D.C.: August 30, 2018.

*High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*. GAO-18-645T. Washington, D.C.: July 25, 2018.

*Information Security: Supply Chain Risks Affecting Federal Agencies*. GAO-18-667T. Washington, D.C.: July 12, 2018.

*Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*. GAO-18-210. Washington, D.C.: March 6, 2018.

*Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*. GAO-18-211. Washington, D.C.: February 15, 2018.

*Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*. GAO-18-175. Washington, D.C.: February 6, 2018.

# Strengthening Department of Homeland Security Management Functions

The Department of Homeland Security (DHS) needs to continue implementing its Integrated Strategy for High-Risk Management with a particular focus on building its capacity in the areas of acquisition, information technology (IT), and financial management.

**Why Area Is High Risk**

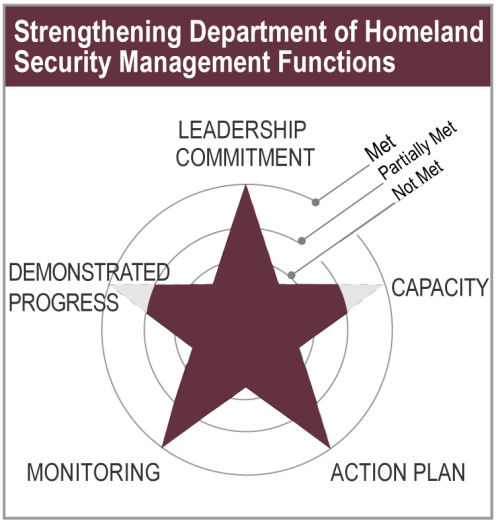
In 2003, we designated implementing and transforming DHS as high risk because the department had to transform 22 agencies—several with major management challenges—into one department. Given the significant effort required to build and integrate a department as large and complex as DHS, our initial high-risk designation addressed the department's implementation and transformation efforts to include associated management and programmatic challenges. Failure to effectively address these challenges could have serious consequences for U.S. national and economic security.

Since 2003, the focus of this high-risk area has evolved in tandem with DHS's maturation and evolution. In September 2011, we reported in our assessment of DHS's progress that the department had implemented key homeland security operations and achieved important goals in many areas but continuing weaknesses in DHS's management functions had been a key theme impacting the department's implementation efforts.

As a result, in our 2013 high-risk update, we narrowed the scope of the high-risk area to strengthening and integrating DHS management functions (human capital, acquisition, information technology, and financial).

**Contact Information**

For additional information about this high-risk area, contact Chris Currie (404) 679-1875 or curriec@gao.gov.




Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, ratings for all five criteria remain unchanged. DHS has continued its efforts to strengthen and integrate its acquisition, information technology, financial, and human capital management functions. It has continued to meet three out of five criteria for removal from the High-Risk List (leadership commitment, action plan, and monitoring) and partially meet the remaining two criteria (capacity and demonstrated progress).

**Leadership commitment: met.** DHS top leadership, including the Secretary and Deputy Secretary of Homeland Security, has continued to demonstrate exemplary commitment and support for addressing the department's management challenges. They have also taken actions to institutionalize this commitment to help ensure the long-term success of the department's efforts. One such effort is the Under Secretary for Management's Integrated Priorities initiative to strengthen the integration of DHS's business operations across the department. During monthly leadership meetings with the Under Secretary for Management, the department's Chief Executive Officers have been providing status updates on their respective actions to address this high-risk designation.

**Capacity: partially met.** With regard to acquisition staffing, DHS has analyzed components' acquisition program staffing assessments but has yet to conduct an in-depth analysis across components or develop a plan to address any gaps.

With regard to IT staffing, DHS has not identified or reported to Congress or the Office of Personnel Management (OPM) on its department-wide cybersecurity specialty areas of critical needs, such as cybersecurity management or incident response, as required by law. In February 2018, we recommended that DHS take steps to ensure that (1) its cybersecurity workforce procedures identify position vacancies and responsibilities, (2)

cybersecurity workforce data are complete and accurate, and (3) plans for reporting critical needs are developed. DHS concurred and stated it planned to provide further evidence addressing the recommendations by the end of the first quarter of fiscal year 2019, which we will assess upon receipt.

With regard to financial management capacity, DHS has continued its efforts to identify and allocate resources for financial management but additional progress is needed. For example, DHS's financial statement auditor has identified several capacity-related issues, including resource limitations and inadequate management and staff training, as causes for the material weaknesses reported.

**Action plan: met.** In January 2011, DHS produced its first Integrated Strategy for High-Risk Management and has issued 14 updated versions, most recently in September 2018. The September 2018 strategy describes DHS's progress to-date and planned corrective actions to further strengthen its management functions. DHS's strategy and approach, if effectively implemented and sustained, provides a path for DHS to be removed from our High-Risk List.

**Monitoring: met.** In the most recent September 2018 Integrated Strategy for High-Risk Management, DHS included performance measures to monitor key management initiatives. For example, DHS monitors the percentage of components demonstrating effective internal controls for significant business processes as a way of gauging progress toward improving financial management. In addition, DHS is also better positioned to monitor its financial system modernization projects since it established a joint program management office in October 2017. This office is to, among other things, centralize program governance and streamline its decision-making processes, and provide DHS management with regular updates on the department's financial system modernization efforts.

**Demonstrated progress: partially met.** In 2010, we identified, and DHS agreed, that achieving 30 specific outcomes would be critical to addressing the challenges within the department's management areas. As of September 2018, DHS has fully addressed 17 of the 30 needed outcomes, mostly addressed 4, partially addressed 6, and initiated actions to address the remaining 3. Since our 2017 High-Risk Report, DHS has taken steps to fully address two human capital outcomes by demonstrating that components are basing hiring decisions and promotions on human capital competencies and strengthening employee

engagement efforts. In addition, DHS has fully addressed two IT outcomes by (1) providing ongoing oversight and support to troubled IT investments to help improve their cost, schedule, and performance; and (2) demonstrating significant progress in implementing its IT strategic workforce planning initiative.

Important progress and work remaining in key areas include:

- Acquisition management. DHS continues to face challenges in funding its acquisition portfolio. In May 2018, we found that recent enhancements to DHS's acquisition management, resource allocation, and requirements policies largely reflect key portfolio management practices. However, we also found that of the 24 major acquisition programs we assessed with approved schedule and cost goals, only 10 were on track to meet those goals during 2017—a decrease from 2016.

  In addition, we found that DHS's portfolio of major acquisition programs is not affordable from fiscal years 2018 to 2022. DHS has taken steps to strengthen requirements development across the department, such as reestablishing the Joint Requirements Council in June 2014. However, opportunities remain to further strengthen DHS's acquisition process by using the Joint Requirements Council to impact DHS's budget. The council could better fulfill its mission by identifying overlapping or common requirements, and by making recommendations to senior leadership to help ensure that DHS uses its finite investment resources wisely, and maintains a balanced portfolio of investments that combine near-term operational improvements with long-term strategic planning.
- IT management. DHS has updated its approach for managing its portfolios of IT investments across all components. As part of the revised approach, the department is utilizing its capital planning and investment control process and the Joint Requirements Council to assess IT investments across the department on an ongoing basis. For example, as part of its capital planning process for the fiscal year 2020 budget, the Office of the Chief Information Officer worked with the components to assess each major IT investment to ensure alignment with DHS's functional portfolios, and to identify opportunities to share capabilities across components. This updated approach should enable DHS to identify potentially duplicative investments and opportunities for consolidating investments, as well as reduce component-specific investments.

Additionally, DHS has continued to take steps to enhance its information security program. In November 2018, the department's financial statement auditor reported that DHS had made progress in correcting its prior year IT security weaknesses. However, for the 15th consecutive year, the auditor designated deficiencies in IT systems controls as a material weakness for financial reporting purposes. Work also remains in implementing our six open recommendations concerning DHS's cybersecurity workforce assessment requirements.

- Financial management. DHS received a clean audit opinion on its financial statements for 6 consecutive years—fiscal years 2013 to 2018. However, its auditor reported two material weaknesses in the areas of financial reporting and information technology controls and financial systems, as well as instances of non-compliance with laws and regulations. These deficiencies hamper DHS's ability to provide reasonable assurance that its financial reporting is reliable and the department is in compliance with applicable laws and regulations. In addition, much work remains to modernize components' financial management systems and business processes.
- Human capital management. DHS has continued to strengthen its employee engagement efforts by implementing our 2012 recommendation to establish metrics of success within components' action plans for addressing its employee satisfaction problems. Further, DHS has conducted audits to better ensure components are basing hiring decisions and promotions on human capital competencies. In addition, OPM's 2018 Federal Employee Viewpoint Survey data showed that in the past 2 years, DHS's score on the Employee Engagement Index (EEI) increased by 4 points—from 56 in 2016 to 60 in 2018—which was 1 point more than the government wide increase over the same period. While this improvement is notable, DHS's current EEI score is 1 point below its EEI baseline score in 2010, suggesting that DHS is still working to regain lost ground after an 8 point drop between 2010 and 2015. DHS has considerable work ahead to improve its employee engagement as its 2018 EEI score ranked 20th among 20 large and very large federal agencies.
- Management integration. Since 2015, DHS has focused its efforts to address crosscutting management challenges through the establishment and monitoring of Integrated Priorities. The department updated these priorities in September 2017. Each priority includes goals, objectives, and measurable action plans that are monitored at monthly leadership meetings led by senior DHS officials, including the Under Secretary for Management. To achieve this outcome, DHS needs to continue to demonstrate sustainable progress integrating its

management functions within and across the department, as well as fully address the other 13 outcomes it has not yet fully achieved.

## What Remains to Be Done

Over the years, we have made hundreds of recommendations related to DHS management functions and many have been implemented. Continued progress for this high-risk area depends primarily on addressing the remaining outcomes. In the coming years, DHS needs to continue implementing its Integrated Strategy for High-Risk Management to show measurable, sustainable progress in implementing corrective actions and achieving outcomes. In doing so, it remains important for DHS to

- maintain its current level of top leadership support and sustained commitment to ensure continued progress in executing its corrective actions through completion;
- continue to identify the people and resources necessary to make progress towards achieving outcomes, work to mitigate shortfalls and prioritize initiatives as needed, and communicate to senior leadership critical resource gaps;
- continue to implement its plan for addressing this high-risk area and periodically provide assessments of its progress to us and Congress;
- closely track and independently validate the effectiveness and sustainability of its corrective actions, and make midcourse adjustments as needed; and
- make continued progress in achieving the 13 outcomes it has not fully addressed and demonstrate that systems, personnel, and policies are in place to ensure that progress can be sustained over time.

## Related GAO Products

*DHS Acquisitions: Additional Practices Could Help Components Better Develop Operational Requirements*. GAO-18-550 Washington, D.C.: August 8, 2018.

*Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management*. GAO-18-339SP Washington, D.C.: May 17, 2018.

*Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*. GAO-18-175, Washington, D.C.: February 6, 2018.

*DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks*. GAO-17-799 Washington, D.C.: September 26, 2017.

*Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed*. GAO-17-284 Washington, D.C.: May 18, 2017.

*Homeland Security Acquisitions: Identifying All Non-Major Acquisitions Would Advance Ongoing Efforts to Improve Management*. GAO-17-396 Washington, D.C.: April 13, 2017.

*Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress*. GAO-17-346SP Washington, D.C.: April 6, 2017.

# Appendix II: Areas Removed From the High-Risk List

The following pages provide overviews of the two areas removed from the High-Risk List. Each overview discusses (1) why the area was high risk, and (2) why the area is being removed from the list. Each of these high-risk areas is also described on our High-Risk List website, http://www.gao.gov/highrisk/overview.

# DOD Supply Chain Management

We are removing this high-risk area because the Department of Defense (DOD) has made sufficient progress on the remaining seven actions and outcomes we recommended for improving supply chain management. Congressional attention, DOD leadership commitment, and our collaboration contributed to this successful outcome.

**Why Area Was High Risk**

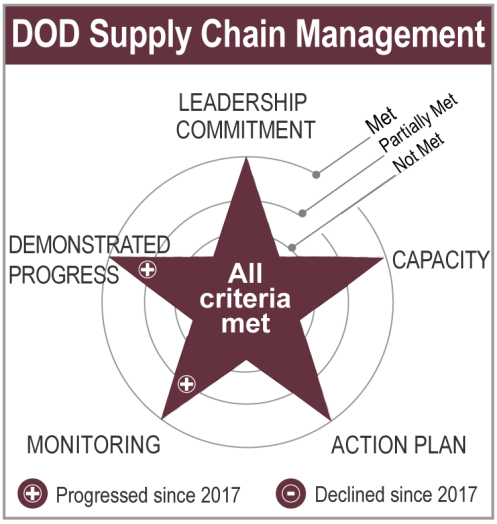
DOD manages about 4.9 million secondary inventory items, such as spare parts, with a reported value of $92.9 billion as of September 2017. Effective and efficient supply chain management is critical for (1) supporting the readiness and capabilities of the force and (2) helping to ensure that DOD avoids spending resources on unneeded inventory that could be better applied to other defense and national priorities. We define supply chain management as including three segments—inventory management, asset visibility, and materiel distribution.

DOD Supply Chain Management has been on our High-Risk List since 1990—starting with inventory management—because of inefficient and ineffective management practices leading to excess inventory. In 2005, we added asset visibility and materiel distribution to this high-risk area due to weaknesses identified during operations in Iraq and Afghanistan, including backlogs of hundreds of pallets and containers at distribution points.

In 2017, we removed inventory management from this area because DOD made key improvements, such as reducing on-order excess inventory by about $600 million and addressing each of our high-risk criteria, resulting in demonstrable and sustained improvements.

**Contact Information**

For additional information about this high-risk area, contact Diana Maurer at 202-512-9627 or maurerd@gao.gov.



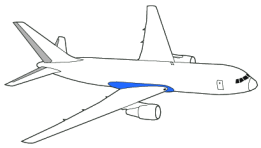

Source: GAO analysis. | GAO-19-157SP

## Why High-Risk Area is Being Removed

From 2014 to 2017, we identified 18 actions and outcomes DOD needed to implement in order for its supply chain management to be removed from our High-Risk List. In our 2017 High-Risk Report, we reported that DOD had made progress in addressing 11 actions and met the criteria of leadership commitment, capacity, and action plan for asset visibility and materiel distribution. However, DOD needed to take additional actions to fully implement the remaining seven actions and outcomes related to the monitoring and demonstrated progress criteria (see figure 6).

**Figure 6: Segments of GAO's Department of Defense's Supply Chain Management High-Risk Area**


**Asset visibility** is DOD's ability to provide timely and accurate information on the location, quantity, condition, movement, and status of its inventory. DOD had weaknesses in maintaining visibility of supplies, such as problems with inadequate radio-frequency identification information to track all cargo movements.



**Materiel distribution** is DOD's ability to operate its global distribution pipeline to deliver the right item, to the right place, at the right time, and at the right cost. DOD faced challenges in delivering supplies and equipment, including meeting delivery standards and timelines for cargo shipments as well as maintaining complete delivery data for surface shipments.

Source: GAO. | GAO-19-157SP

We are removing DOD Supply Chain Management from the High-Risk List because, since 2017, DOD has addressed the remaining two criteria (monitoring and demonstrated progress) for asset visibility and materiel distribution by addressing the seven actions and outcomes identified in our 2017 High-Risk Report.

## Asset Visibility


Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, DOD has continued to meet the criteria of leadership commitment, capacity, and action plan for asset visibility. Further, DOD has fully addressed the three remaining actions and outcomes we outlined in 2017 in order to mitigate or resolve long-standing weaknesses in asset visibility. Consequently, DOD has met the monitoring and demonstrated progress criteria for asset visibility to remove this area from our High-Risk List.

**Leadership commitment: met.** Senior leaders have continued to demonstrate commitment through their involvement in groups such as the Supply Chain Executive Steering Committee—senior-level officials responsible for overseeing asset visibility improvement efforts—and through the Asset Visibility Working Group, which identifies opportunities for improvement and monitors the implementation of initiatives by issuing its Strategy for Improving DOD Asset Visibility (Strategy) in 2014, 2015, and 2017.

**Capacity: met.** DOD continues to demonstrate that it has the capacity—personnel and resources—to improve asset visibility. For example, DOD's 2015 and 2017 Strategies advise the components to consider items such as staffing, materiel, and sustainment costs when documenting cost estimates for the initiatives in the Strategy, as we recommended in January 2015.

**Action plan: met.** A provision in the National Defense Authorization Act for Fiscal Year 2014 required DOD to submit to Congress a comprehensive strategy and implementation plans for improving asset tracking and in-transit visibility. In January 2014, DOD issued the Strategy and accompanying implementation plans, which outlined initiatives intended to improve asset visibility. DOD updated its 2014 Strategy in October 2015 and in August 2017.

Importantly, since 2017 DOD addressed the three remaining actions and outcomes related to the monitoring and demonstrated progress criteria through updates to and implementation of the Strategies (see table 7).

**Table 7: Status of Asset Visibility Remaining Action Items Required to Remove Supply Chain Management from GAO's High-Risk List**

| Action items | | Action item status | High-risk category |
|---|---|---|---|
| 1. | Incorporate the attributes of successful performance measures (e.g., clear, quantifiable, objective, and reliable), as appropriate, in subsequent updates to the Strategy for Improving DOD Asset Visibility | Met | Monitoring |
| 2. | Take steps to incorporate into after-action reports information relating to performance measures for the asset visibility initiatives | Met | Monitoring |
| 3. | Demonstrate sustained progress in implementing initiatives that result in measurable outcomes and progress towards realizing the goals and objectives in the Strategy for Improving DOD Asset Visibility | Met | Demonstrated progress |

Source: GAO analysis and prior GAO report. | GAO-19-157SP

**Monitoring: met.** DOD provided guidance in its 2017 update to the Strategy for the military components to consider key attributes of successful performance measures during metric development for their improvement initiatives. As appropriate, the military components have followed the guidance and provided high-level summary metrics updates to the Asset Visibility Working Group. In addition, DOD has taken steps to monitor asset visibility by incorporating into after-action reports, as appropriate, information relating to performance measures. These after-action reports serve as closure documents and permanent records of each initiative's accomplishments.

**Demonstrated progress: met.** DOD has demonstrated sustained progress by completing 34 of the 39 initiatives to improve asset visibility and continues to monitor the remaining 5 initiatives. These initiatives have supported DOD's goals and objectives, which include: (1) improving visibility efficiencies of physical inventories, receipt processing, cargo tracking, and unit moves; (2) ensuring asset visibility data are discoverable, accessible, and understandable to support informed decision-making across the enterprise; and (3) increasing efficiencies for delivery accuracy and cycle times. Also, the Asset Visibility Working Group meets regularly to identify opportunities to further improve asset visibility within DOD.

DOD has taken the following actions to demonstrate sustained progress: (1) created an integrated single portal system providing 7,500 users access to near-real-time, in-transit visibility of eight million lines of items of supply and transportation data; and (2) increased its visibility of assets through radio-frequency identification (RFID), an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. There are two main types of RFID tags,

passive and active, which show whether assets are in-storage, in-transit, in-process, or in-use. Passive tags, such as mass transit passes, do not contain their own power source and cannot initiate communication with a reader; while active tags, such as an “E-Z pass,” contain a power source and a transmitter, and send a continuous signal over longer distances.

DOD closed nine initiatives from its Strategies by implementing RFID technology. For example, the Marine Corps implemented long-range passive RFID for visibility and accountability of items, resulting in improvements that include an increased range for “reading” an item—from 30 feet to 240 feet—and reduced inventory cycle times from 12 days to 10 hours. Also, the Navy reported that the use of passive RFID technology to support the overhaul of its nuclear-powered attack submarines enabled the Navy to better track parts, resulting in 98 percent fewer missing components and an average cost avoidance of $1.3 million per boat.

Additionally, according to DOD, the use of RFID tags to provide visibility of sustainment cargo at the tactical leg resulted in $1.4 million annual cost savings. Further, DOD reported that the migration of the active RFID enterprise from a proprietary communication standard to a competitive multivendor environment reduced the cost of active RFID tags by half, resulting in an estimated $5.7 million annual reduction in costs.

## Materiel Distribution


Source: GAO analysis. | GAO-19-157SP

Since our 2017 High-Risk Report, DOD has continued to meet the criteria of leadership commitment, capacity, and action plan for materiel distribution. Further, DOD has fully addressed the four remaining actions and outcomes we outlined in 2017 in order to mitigate or resolve long-standing weaknesses in materiel distribution. Consequently, DOD has met the monitoring and demonstrated progress criteria for materiel distribution to remove this area from our High-Risk List.

**Leadership commitment: met.** Senior leaders continue to demonstrate commitment through their involvement in groups such as the Supply Chain Executive Steering Committee—senior-level officials responsible for overseeing materiel distribution corrective actions—and through the Distribution Working Group, which helped develop the Materiel Distribution Improvement Plan (Improvement Plan) in 2016.

**Capacity: met.** DOD has continued to demonstrate that it has the personnel and resources, such as key organizations and the associated

governance structure, to improve materiel distribution. The Improvement Plan recognizes that additional resources will be required to accomplish its corrective actions and close any identified performance gaps within the time frame specified.

**Action plan: met.** In 2016, DOD developed its corrective action plan to address the department's materiel distribution challenges. The Improvement Plan details specific goals and actions to better measure the end-to-end distribution process, ensure the accuracy of underlying data, and strengthen and integrate distribution policies and the governance structure.

Importantly, since 2017, DOD has fully addressed the four remaining actions and outcomes related to monitoring and demonstrated progress to mitigate or resolve long-standing weaknesses in materiel distribution (see table 8).

**Table 8: Status of Materiel Distribution Remaining Action Items Required to Remove Supply Chain Management from GAO's High-Risk List**

| Action items | | Action item status | High-risk category |
|---|---|---|---|
| 1. | Make progress in developing Department of Defense's (DOD's) suite of distribution performance metrics, improving the quality of data underlying those metrics, and sharing metrics information among stakeholders. | Met | Monitoring |
| 2. | Integrate distribution metrics data, including cost data, from the combatant commands and other DOD components, as appropriate, on the performance of all legs of the distribution system, including the tactical leg.[a] | Met | Monitoring |
| 3. | Refine existing actions in the Materiel Distribution Improvement Plan or incorporate additional actions based on interim progress and results, and update the Materiel Distribution Improvement Plan accordingly. | Met | Monitoring |
| 4. | Demonstrate that the actions implemented under its Materiel Distribution Improvement Plan improve its capability to comprehensively measure distribution performance, identify distribution problems and root causes, and identify and implement solutions. | Met | Demonstrated progress |

Source: GAO analysis and prior GAO report. | GAO-19-157SP

[a]The tactical leg is the last segment of the distribution system between the supply points in a military theater of operations and the forward operating bases and units.

**Monitoring: met.** DOD has monitored materiel distribution by making progress in developing its suite of distribution performance metrics, improving the quality of their underlying data, and sharing metrics information with stakeholders. For example, in January 2017, DOD developed a suite of performance metrics that provides a comprehensive picture of the distribution process, including whether supplies are

delivered on time and at sufficient quantity and quality. Also, DOD implemented checklists to assess the quality of data underlying each performance metric based on relevance, accuracy, comparability, and interpretability.

The checklists and their standards assist in identifying root causes and addressing areas where performance data quality may be lacking. DOD has also incorporated internal control requirements in its supply chain management guidance to increase confidence in the performance data. Additionally, DOD has revised its policy documents to require stakeholders to routinely capture and share distribution performance metrics, including cost data, and the department maintains websites to provide current performance information to distribution stakeholders.

DOD has also incorporated distribution metrics, as appropriate, on the performance of all legs of the distribution system, including the tactical leg (i.e., the last segment of the distribution system). We previously reported on DOD's deficiencies to accurately assess its distribution performance at the tactical leg, such as missing delivery dates for shipments in Afghanistan. Since that time, the geographic combatant commands have been tracking metrics at the tactical leg, including required delivery dates, to determine the movement and causes of delays for shipments, and have been sharing distribution performance information with the U.S. Transportation Command (TRANSCOM) through their deployment and distribution operations centers. DOD is implementing a cost framework to incorporate transportation costs for all legs of the distribution system, which will provide an additional metric for distribution stakeholders to assess the efficiency of the system. The first phase of the cost framework began operating in August 2018 and is expected to be fully implemented in 2019.

DOD is making progress in refining its Improvement Plan and is incorporating additional actions based on interim progress and results. Since DOD issued the Improvement Plan in September 2016, the agency has (1) documented the results and monitored the status of each corrective action, (2) revised completion dates as needed, and (3) periodically provided decision makers with summary action charts, plans, and milestones. DOD is also updating its instruction on management and oversight of the distribution enterprise to clarify the roles and responsibilities of all distribution stakeholders. DOD officials have not determined a date for when this instruction will be issued.

**Demonstrated progress: met.** DOD has demonstrated sustained progress in improving its capability to comprehensively measure distribution performance, identify distribution problems and root causes, and implement solutions. DOD has implemented 10 of 18 corrective actions in its Improvement Plan and is on track to implement the

remaining 8 by September 2019. Because of this progress, DOD's monthly shipment reports have assessed performance against enhanced metrics across the distribution system. For example, in December 2017, TRANSCOM investigated performance standards for truck deliveries from its Defense Logistics Agency warehouses in Bahrain to customers in Kuwait due to frequent delays in shipments. TRANSCOM determined that inadequate time for clearing customs in Kuwait resulted in an unrealistic delivery standard.

TRANSCOM, in coordination with distribution stakeholders, adjusted the delivery standard to adequately account for the in-theater customs process. In addition, TRANSCOM, in partnership with the Defense Logistics Agency and the General Services Administration, developed and implemented initiatives focused on distribution process and operational improvements to reduce costs and improve distribution services to the warfighter. According to DOD, these efforts have resulted in at least $1.56 billion in distribution cost avoidances to date.

## Monitoring After Removal

DOD has demonstrated commendable, sustained progress improving its supply chain management. This does not mean DOD has addressed all risk within this area. It remains imperative that senior leaders continue their efforts to implement initiatives and corrective actions to maintain visibility of supplies, track cargo movements, meet delivery standards, and maintain delivery data for shipments. Continued oversight and attention are also warranted given the recent reorganization of the Office of the Under Secretary of Defense for Acquisition and Sustainment and the resulting change in the oversight structure of Supply Chain Management. We will therefore continue to conduct oversight of supply chain management at DOD.

## Related GAO Products

*Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*. GAO-17-183. Washington, D.C.: Mar. 16, 2017.

*Defense Logistics: DOD Has Addressed Most Reporting Requirements and Continues to Refine its Asset Visibility Strategy*. GAO-16-88. Washington, D.C.: Dec. 22, 2015.

*Defense Logistics: Improvements Needed to Accurately Assess the Performance of DOD's Materiel Distribution Pipeline*. GAO-15-226. Washington, D.C.: Feb. 26, 2015.

# Mitigating Gaps in Weather Satellite Data

We are removing this high-risk area because—with strong congressional support and oversight—the National Oceanic and Atmospheric Administration (NOAA) and the Department of Defense (DOD) have made significant progress in establishing and implementing plans to mitigate potential gaps in weather satellite data.

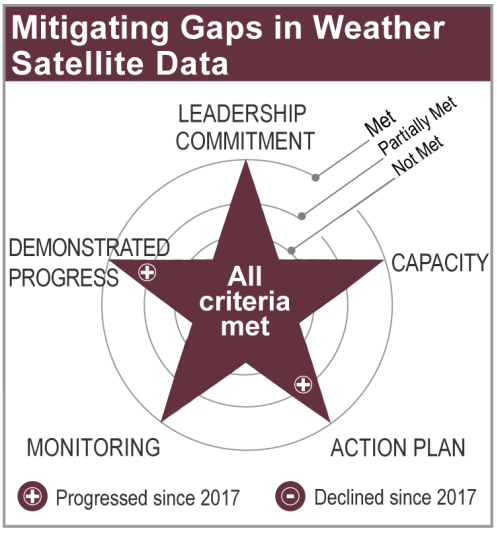
**Why Area Was High Risk**

The United States relies on two satellite systems for weather forecasts and observations: (1) polar-orbiting satellites that provide a global perspective every morning and afternoon and (2) geostationary satellites that maintain a fixed view of the nation. NOAA is responsible for the polar satellite program that crosses the equator in the afternoon and for the geostationary satellite program. DOD is responsible for the polar satellite program that crosses the equator in the early morning orbit. These agencies are planning or executing major satellite acquisition programs to replace existing polar and geostationary satellites that are nearing the end of, or are beyond, their expected life spans.

A gap in satellite data would result in less accurate and timely weather forecasts and warnings of extreme events—such as hurricanes and floods. Given the criticality of satellite data to weather forecasts, the likelihood of significant gaps in weather satellite data, and the potential impact of such gaps on the health and safety of the U.S. population and economy, we concluded that the potential gap in weather satellite data was a high-risk area and added it to the High-Risk List in 2013. More recently, in recognition of NOAA's progress, we removed the geostationary satellite segment from the high-risk area in 2017.

**Contact Information**

For additional information about this high-risk area, contact Carol C. Harris at 202-512-4456 or at harriscc@gao.gov.




Source: GAO analysis. | GAO-19-157SP

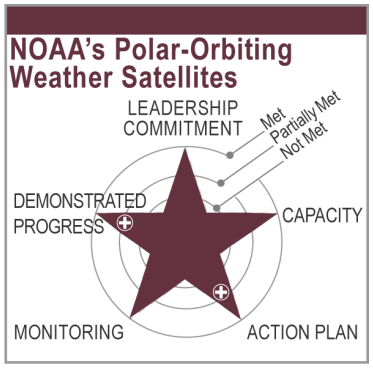
**Why High-Risk Area Is Being Removed**

In our 2017 High-Risk Report, we reported that NOAA had fully implemented criteria associated with demonstrating leadership commitment, having the needed capacity to address risks, and monitoring progress.

We also reported that NOAA had partially implemented the criteria for establishing an action plan and demonstrating progress. In addition, our 2017 report noted DOD's slow progress in establishing plans for its follow-on weather satellite program and for determining how it would fulfill other weather requirements in the early morning orbit.

Since that time, (1) NOAA has fully implemented actions in response to the remaining two criteria that had previously been partially implemented and (2) DOD, pursuant to statutes and accompanying congressional direction, established and began implementing plans both for its follow-on weather satellite program and for addressing the key requirements that were not included in that satellite program. Consequently, we are removing the need to mitigate gaps in weather satellite data from our High-Risk List.

# NOAA's Polar-Orbiting Weather Satellites




Source: GAO analysis. | GAO-19-157SP

Since our last high-risk update in 2017, NOAA continues to meet the criteria of leadership commitment, capacity, and monitoring and now also meets the criteria of action plan and demonstrated progress.

**Leadership commitment: met.** NOAA program officials met the leadership commitment criteria in 2015 and have continued to sustain their strong leadership commitment to mitigating potential satellite data gaps since that time. For example, NOAA issued and frequently updated its polar satellite gap mitigation plan, which identifies the specific technical, programmatic, and management steps the agency is taking to ensure that satellite mitigation options are viable. In addition, NOAA executives continue to oversee the acquisition of polar-orbiting satellites through monthly briefings on the cost, schedule, and risks affecting the satellites' development.

**Capacity: met.** NOAA continues to meet the criterion of improving its capacity to address the risk of a satellite data gap. In December 2014, we recommended that NOAA investigate ways to prioritize the gap mitigation projects with the greatest potential benefit to weather forecasting, such as by improving its high-performance computing capacity. NOAA agreed with this recommendation and implemented it. For example, NOAA upgraded its high-performance computers, which allowed the agency to move forward on multiple other mitigation activities, including experimenting with other data sources and assimilating these data into its weather models.

**Action plan: met.** NOAA now meets the criterion for having a plan to address the risk of a polar satellite data gap, which is an increase over its rating in 2017. In June 2012, we reported that, while NOAA officials communicated publicly and often about the risk of a polar satellite data gap, the agency had not established plans to mitigate the gap. We recommended that NOAA establish a gap mitigation plan, and the agency did so in February 2014. However, in December 2014, we recommended that NOAA revise its plan to address shortfalls, including (1) adding recovery time objectives for key products, (2) identifying opportunities for accelerating the calibration and validation of satellite data products, (3) providing an assessment of available alternatives based on their costs

and impacts, and (4) establishing a schedule with meaningful timelines and linkages among mitigation activities.

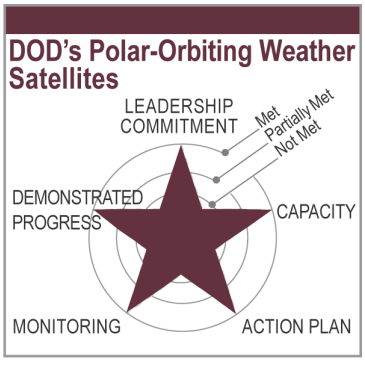
The agency agreed with the recommendation and subsequently addressed it. Specifically, NOAA issued three updates to its gap mitigation plan between January 2016 and February 2017. With the last of the updates, the agency addressed the shortfalls we had identified.

**Monitoring: met.** NOAA met this criterion in 2017, and continues to meet it now, by implementing our recommendations to more consistently and comprehensively monitor its progress on gap mitigation activities. For example, all three NOAA organizations responsible for gap mitigation projects regularly brief senior management on their progress.

**Demonstrated progress: met.** NOAA now meets the criterion for demonstrated progress, which is an increase over its prior rating. In our 2017 High-Risk Report, we noted that NOAA had identified 35 different gap mitigation projects and was making progress in implementing them. These projects fell into three general categories: (1) understanding the likelihood and impact of a gap, (2) reducing the likelihood of a gap, and (3) reducing the impact of a gap. Nevertheless, one of the most important steps in reducing the likelihood of a gap—keeping the launch of the next polar satellite on schedule—had encountered problems. Specifically, agency officials decided to delay the launch due to challenges in developing the ground system and a critical instrument on the spacecraft. This delay exacerbated the probability of a satellite data gap.

More recently, however, NOAA was able to demonstrate progress by successfully launching the satellite in November 2017. That satellite, now called NOAA-20, is currently operational and is being used to provide advanced weather data and forecasts. Moreover, the agency is also working to build and launch the next satellites in the polar satellite program.

## DOD's Polar-Orbiting Weather Satellites




Source: GAO analysis. | GAO-19-157SP

Since our last high-risk update in 2017, DOD now meets all five high-risk criteria.

**Leadership commitment: met.** With strong congressional oversight, DOD now meets this criterion. Pursuant to enactment of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for

Fiscal Year 2015 (NDAA for FY 2015), the National Defense Authorization Act for Fiscal Year 2016 (NDAA for FY 2016), and the Consolidated Appropriations Act, 2016, DOD leadership committed to developing and implementing plans to address its weather satellite requirements. For example, in late 2017, the department awarded a contract for its Weather System Follow-on—Microwave satellite to fulfill core weather requirements.

**Capacity: met.** With strong congressional oversight, DOD now meets the capacity criterion. Specifically, the NDAA for FY 2015 restricted the availability of 50 percent of the FY 2015 funds authorized for the Weather Satellite Follow-on System (now called the Weather System Follow-on—Microwave satellite program) until DOD submitted to the congressional defense committees a plan to meet weather monitoring data collection requirements. In addition, the explanatory statement that accompanied the Consolidated Appropriations Act, 2016, recommended that the Air Force focus on ensuring that the next generation of weather satellites meet the full spectrum of requirements and work with civil stakeholders to leverage appropriate civil or international weather assets.

As called for in the law and the explanatory statement, DOD established plans to meet weather monitoring data collection needs, including by acquiring satellites as part of a family of systems to replace its aging legacy weather satellites. Additionally, DOD formally coordinated with NOAA on weather monitoring data collection efforts. In January 2017, the Air Force and NOAA signed a memorandum of agreement, and in November 2017, signed an annex to that agreement, to allow for the exchange of information and collaboration on a plan for collecting weather monitoring data. The Air Force and NOAA are now developing plans to relocate a residual NOAA satellite over the Indian Ocean, an area of concern for cloud characterization and area-specific weather imagery coverage.

**Action plan: met.** In our 2017 High-Risk Report, we reported that DOD was slow to establish plans for its Weather System Follow-on–Microwave program and had made little progress in determining how it would meet weather satellite requirements for cloud characterization and area-specific weather imagery. Pursuant to the NDAA for FY 2015, the NDAA for FY 2016, and the explanatory statement that accompanied the Consolidated Appropriations Act, 2016, the department developed and began implementing plans to address its weather satellite requirements. As mentioned above, in late 2017, the department awarded a contract for its Weather System Follow-on–Microwave satellite to fulfill core weather

requirements. Under this program, the department may launch a demonstration satellite in 2021 and plans to launch an operational satellite in 2022.

DOD also developed plans for providing its two highest-priority capabilities—cloud characterization and area-specific weather imagery data collection—that will not be covered by the Weather System Follow-on–Microwave satellite program. The department is planning a longer-term solution, called the Electro-Optical/Infrared Weather Systems program, to meet these needs, with a planned satellite launch in 2024. Meanwhile, DOD is in the process of acquiring a small prototype satellite, called the Operationally Responsive Space-8 satellite, to provide interim capabilities. DOD plans to launch Operationally Responsive Space-8 as early as 2022.

**Monitoring: met.** DOD now meets the monitoring criterion as evidenced by its actions to initiate a major acquisition program, the Weather System Follow-on–Microwave, and award a contract for the first satellite. In addition, program officials stated that they plan to monitor the program's progress toward addressing critical needs and assess its operations and sustainment costs.

**Demonstrated progress: met.** DOD now meets the demonstrated progress criterion because it has developed plans and taken actions to address gaps in weather data through its plans to launch the Weather System Follow-on–Microwave satellite in 2022. The department also plans to launch the Electro-Optical/Infrared Weather Systems satellite in 2024 and provide interim capabilities beginning as early as 2022. By developing these plans, DOD has reduced the risk of a gap in weather satellite data and addressed the concerns about a lack of planning that we identified in our 2017 High-Risk Report. DOD's effective implementation of its plans will be key to further reducing the risks of gaps in weather satellite data in the future.

## Monitoring After Removal

Moving forward, we will continue to monitor both NOAA and DOD efforts to develop and launch the next satellites in their respective weather satellite programs. NOAA plans to launch its next geostationary weather satellite in 2021 and to launch its next polar weather satellite in 2022. DOD plans satellite launches in 2021 (potentially), 2022, and 2024. In addition, we will continue to monitor DOD's efforts to develop long-term plans to meet its weather satellite requirements.

## Related GAO Products

*Weapon Systems Annual Assessment: Knowledge Gaps Pose Risks to Sustaining Recent Positive Trends*. GAO-18-360SP. Washington, D.C.: Apr. 25, 2018.

*Satellite Acquisitions: Agencies May Recover a Limited Portion of Contract Value When Satellites Fail*. GAO-17-490. Washington, D.C.: June 9, 2017.

*Defense Acquisitions: Assessments of Selected Weapon Programs*. GAO-17-333SP. Washington, D.C.: Mar. 30, 2017.

*Defense Weather Satellites: DOD Faces Acquisition Challenges for Addressing Capability Needs*. GAO-16-769T. Washington, D.C.: July 7, 2016.

*Polar Satellites: NOAA Faces Challenges and Uncertainties that Could Affect the Availability of Critical Weather Data*. GAO-16-773T. Washington, D.C.: July 7, 2016.

*Polar Weather Satellites: NOAA Is Working to Ensure Continuity but Needs to Quickly Address Information Security Weaknesses and Future Program Uncertainties*. GAO-16-359. Washington, D.C.: May 17, 2016.

*Defense Weather Satellites: Analysis of Alternatives Is Useful for Certain Capabilities, but Ineffective Coordination Limited Assessment of Two Capabilities*. GAO-16-252R. Washington, D.C.: Mar. 10, 2016

## GAO's Mission

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

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

## Order by Phone

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

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

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

## Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

## Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

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

## Strategic Planning and External Liaison

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