United States Government Accountability Office

Report to Congressional Committees

November 2018

U.S. SECRET SERVICE

Action Needed to Address Gaps in IT Workforce Planning and Management Practices

Accessible Version

GAO-19-60

November 2018

U.S. SECRET SERVICE

Action Needed to Address Gaps in IT Workforce Planning and Management Practices

GAO Highlights

Highlights of GAO-19-60, a report to congressional committees

Why GAO Did This Study

Commonly known for protecting the President, the Secret Service also plays a leading role in investigating and preventing financial and electronic crimes. To accomplish its mission, the Secret Service relies heavily on the use of IT infrastructure and systems. In 2009, the component initiated the IITT investment—a portfolio of programs and projects that are intended to, among other things, improve systems availability and security in support of the component's business operations.

GAO was asked to review the Secret Service's oversight of its IT portfolio and workforce. This report discusses the extent to which the (1) CIO implemented selected IT oversight responsibilities, (2) Secret Service implemented leading IT workforce planning and management practices, and (3) Secret Service and DHS implemented selected performance monitoring practices for IITT. GAO assessed agency documentation against 14 selected component CIO responsibilities established in DHS policy; 15 selected leading workforce planning and management practices within 5 topic areas; and two selected leading industry project monitoring practices that, among other things, were, in GAO's professional judgment, of most significance to managing IITT.

What GAO Recommends

GAO is making 13 recommendations, including that the Secret Service establish a process that ensures the CIO reviews all IT contracts, as appropriate; and identify the skills needed for its IT workforce. DHS concurred with all recommendations and provided estimated dates for implementing each of them.

View GAO-19-60. For more information, contact Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov.

What GAO Found

The U.S. Secret Service (Secret Service) Chief Information Officer (CIO) fully implemented 11 of 14 selected information technology (IT) oversight responsibilities, and partially implemented the remaining 3. The CIO partially implemented the responsibilities to establish a process that ensures the Secret Service reviews IT contracts; ensure that the component's IT policies align with the Department of Homeland Security's (DHS) policies; and set incremental targets to monitor program progress. Additional efforts to fully implement these 3 responsibilities will further position the CIO to effectively manage the IT portfolio.

Of the 15 selected practices within the 5 workforce planning and management areas, the Secret Service fully implemented 3 practices, partly implemented 8, and did not implement 4 (see table). Within the strategic planning area, the component partly implemented the practice to, among other things, develop IT competency needs. While the Secret Service had defined general core competencies for its workforce, the Office of the CIO (OCIO) did not identify all of the technical competencies needed to support its functions. As a result, the office was limited in its ability to address any IT competency gaps that may exist. Also, while work remains to improve morale across the component, the Secret Service substantially implemented the employee morale practices for its IT staff.

The U.S. Secret Service's Implementation of 15 Selected Leading Practices Associated with 5 Workforce Planning and Management Areas for Its Information Technology Workforce

Workforce area	Overall area rating	Number of practices fully implemented	Number of practices partly implemented	Number of practices not implemented
1. Strategic planning	Minimally implemented	0	2	1
2. Recruitment and hiring	Minimally implemented	0	1	2
3. Training and development	Minimally implemented	0	2	1
4. Employee morale	Substantially implemented	2	1	0
5. Performance management	Substantially implemented	1	2	0
Total		**3**	**8**	**4**

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

Secret Service officials said the gaps in implementing the workforce practices were due to, among other things, their focus on reorganizing the IT workforce within OCIO. Until the Secret Service fully implements these practices for its IT workforce, it may be limited in its ability to ensure the timely and effective acquisition and maintenance of the component's IT infrastructure and services.

Of the two selected IT project monitoring practices, DHS and the Secret Service fully implemented the first practice to monitor the performance of the Information Integration and Technology Transformation (IITT) investment. In addition, for the second practice—to monitor projects on incremental development metrics—the Secret Service fully implemented the practice on one of IITT's projects and partially implemented it on another. In particular, OCIO did not fully measure post-deployment user satisfaction with the system on one project. OCIO plans to conduct a user satisfaction survey of the system by September 2018, which should inform the office on whether the system is meeting users' needs.

Contents

Tables

Figures

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FY	fiscal year
IT	information technology
IITT	Information Integration and Technology Transformation
OCIO	Office of the Chief Information Officer
Secret Service	United States Secret Service

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 15, 2018

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael McCaul
Chairman
The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Commonly known for protecting the President, the United States Secret Service (Secret Service), a component of the Department of Homeland Security (DHS), also plays a leading role in investigating and preventing a variety of financial and electronic crimes. For example, the Secret Service's criminal investigation activities encompass financial and electronic crimes, such as identity theft, counterfeiting, and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure. In addition, its protective intelligence efforts include investigating threats against protected persons and facilities, such as the President and the White House. The Secret Service is also responsible for certain security activities, including presidential inaugurations and national conventions.

To accomplish its mission, the Secret Service relies heavily on the use of information technology (IT) infrastructure and communications systems. The component's Chief Information Officer (CIO)[1] plays a key role in effectively managing this infrastructure and systems. Among other things, the CIO is responsible for IT strategic planning and the management and governance of the IT programs and infrastructure. The CIO is also responsible for managing the component's IT workforce, which officials

[1]Throughout this report, CIO and OCIO respectively refer to the Secret Service Chief Information Officer and the Secret Service Office of the Chief Information Officer, unless otherwise specified.

from the Office of the CIO (OCIO) define as the government employees who provide direct and indirect support of the day-to-day operations of the Secret Service's enterprise systems and services.

However, the Secret Service has faced longstanding challenges in managing its IT environment. For example, a National Security Agency audit of the environment in 2008 identified network and system vulnerabilities that needed immediate remediation to protect the Secret Service's systems and electronic information.

To address the challenges with its IT environment, the Secret Service initiated the Information Integration and Technology Transformation (IITT) investment in 2009. IITT is a portfolio of programs and projects that are intended to, among other things, modernize and enhance the IT network infrastructure; provide hardware and software to ensure reliable and consistent voice, data, and radio coverage for Secret Service agents; and provide counterintelligence and data mining capabilities to improve officials' ability to perform the component's investigative mission.

Yet, the Secret Service's implementation of the IITT investment has also been problematic. For example, in 2011, DHS's Office of Inspector General reported that, among other things, the component's schedule for implementing IITT was not realistic.[2] Also in that 2011 report, the Inspector General stated that, while the Secret Service had implemented an internal governance approach for IITT (including establishing governance policies and procedures), it had not implemented a formal department-level IT governance mechanism to provide integrated feedback and direction for the investment.

Given the importance of effective IT management for achieving the Secret Service's mission, you asked us to review the role of the Secret Service CIO in overseeing the component's IT portfolio and workforce. Our specific objectives were to evaluate the extent to which: (1) the Secret Service CIO has implemented selected IT oversight responsibilities, (2) the Secret Service has implemented leading workforce planning and management practices for its IT workforce, and (3) the Secret Service and DHS have implemented selected performance and progress monitoring practices for the IITT investment.

[2]DHS Office of Inspector General, *U.S. Secret Service's Information Technology Modernization Effort (Redacted)*, OIG-11-56 (Mar. 15, 2011).

To address the first objective, we analyzed DHS's policies and guidance on IT management to identify the responsibilities that were to be implemented by the component-level CIO related to overseeing the Secret Service's IT portfolio, including existing systems, acquisitions, and investments.[3] From the list of 33 responsibilities that we identified, we then excluded the responsibility that was associated with information security, which is expected to be addressed as part of a separate, subsequent GAO review. We also excluded those responsibilities that were significantly large in scope (e.g., implement an enterprise architecture) or that, in our professional judgment, lacked specificity (e.g., provide timely delivery of mission IT services). As a result, we excluded from consideration for this review a total of 10 CIO responsibilities.

For the 23 that remained, we then combined certain responsibilities that overlapped with other related responsibilities. For example, we combined related responsibilities on the component CIO's review of IT contracts. As a result, we were left with 14 responsibilities that were relevant for our review. We then validated with the acting DHS CIO that these were key responsibilities for the department's component-level CIOs. Following this validation, we elected to include all 14 of the responsibilities in our review. Appendix I identifies the 14 selected component-level CIO responsibilities.

We then assessed relevant Secret Service documentation to determine the extent to which the CIO had implemented the selected responsibilities. For example, we assessed monthly program management reports demonstrating the CIO's oversight of IT programs, projects, and systems; systems engineering life cycle technical review briefings; the Secret Service's enterprise governance policy; and meeting minutes from the DHS boards and councils on which the CIO participated. We also selected and analyzed two random, non-generalizable samples of a total of 33 IT contracts that the Secret Service awarded between

[3]These policies and guidance included: DHS, Instruction 102-01-004, *Agile Development and Delivery for Information Technology* (April 2016); Instruction 102-02-001, *Capital Planning and Investment Control Guidebook* (March 2016); Directive 102-02, *Capital Planning and Investment Control* (February 2016); Instruction 102-01-103, *Systems Engineering Life Cycle* (November 2015); and Directive 142-02, *Information Technology Integration and Management* (February 2014 and updated in April 2018).

October 1, 2016, and June 30, 2017,[4] as well as the associated approval documentation, to determine whether or not the CIO or the CIO's delegate had approved each of the contracts.

Further, we interviewed Secret Service officials, including the CIO and Deputy CIO, regarding the CIO's implementation of the 14 selected component-level responsibilities. We assessed the evidence against the selected responsibilities to determine the extent to which the CIO had implemented the responsibilities.

To address the second objective, we first identified seven topic areas associated with human capital management based on our review of IT workforce[5] planning and management guidance issued by the Office of Personnel Management, the Chief Human Capital Officers Council, DHS, the Secret Service, and us.[6] Among these topic areas, we then selected five areas that, in our professional judgment, were of particular importance to successful workforce planning and management. These areas are: (1) strategic planning, (2) recruitment and hiring, (3) training and development, (4) employee morale, and (5) performance management.

We also reviewed these same sources and identified numerous leading practices associated with the five topic areas. Among these leading

[4]The first sample included 12 contracts that we selected from a list of 42 IT contracts identified by Secret Service officials. The second sample included 21 contracts that we selected from a list of 86 Secret Service IT contracts identified in the Federal Procurement Data System – Next Generation. Appendix I describes our contract selection methodology in more detail.

[5]As defined by Secret Service OCIO officials, the IT workforce includes government employees who provide direct and indirect support of the day-to-day operations of the component's enterprise systems and services.

[6]5 C.F.R. pt. 250, subpt. B.; GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016); *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans*, GAO-12-940 (Washington, D.C.: Sept. 28, 2012); *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government (Supersedes* GAO-03-893G*),* GAO-04-546G (Washington, D.C.: Mar. 1, 2004); and *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success,* GAO-03-488 (Washington, D.C.: Mar. 14, 2003); Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative* (Sept. 2008); DHS, Instruction 102-01-001*, Acquisition Management Instruction* (Mar. 9, 2016); and the U.S. Secret Service, *Acquisition Workforce Certification,* ADM-10 (04) (Dec. 19, 2012).

practices, we then selected three practices within each of the five areas, for a total of 15 practices. The selected practices were foundational practices that, in our professional judgment, were of particular importance to successful workforce planning and management. Appendix I identifies the five workforce areas and the 15 associated practices that we selected.

We then assessed the Secret Service's workforce planning documentation against the 15 selected leading practices. For example, we analyzed the staffing model that the Secret Service used to determine the number of IT staff it needed, as well as recruitment plans and action plans for improving employee morale. We also interviewed Secret Service officials—including the CIO, Deputy CIO, and workforce planning staff—about the component's efforts to implement the selected leading practices for its IT workforce.

Regarding our assessments of the Secret Service's implementation of the 15 selected leading workforce planning and management practices, we assessed a practice as being fully implemented if component officials provided supporting documentation that demonstrated all aspects of the practice. We assessed a practice as not implemented if the officials did not provide any supporting documentation for that practice, or if they provided documentation that did not demonstrate any aspect of the practice. We assessed a practice as being partly implemented if the officials provided supporting documentation that demonstrated some, but not all, aspects of the selected practice.

In addition, related to our assessments of the Secret Service's implementation of the five selected overall workforce areas, we assessed each area as follows, based on the implementation of the three selected practices within each area:

- *Fully implemented:* The Secret Service provided evidence that it had fully implemented all three of the practices within the workforce area;
- *Substantially implemented:* The Secret Service provided evidence that it had either
  - fully implemented two practices and partly implemented the remaining one practice within the workforce area, or
  - fully implemented one practice and partly implemented the remaining two practices within the workforce area;

- *Partially implemented:* The Secret Service provided evidence that it had partly implemented each of the three practices within the workforce area;
- *Minimally implemented:* The Secret Service provided evidence that it had either
  - partly implemented two practices and not implemented the remaining one practice within the workforce area, or
  - partly implemented one practice and not implemented the remaining two practices within the workforce area; or
- *Not implemented:* The Secret Service did not provide evidence that it had implemented any of the three practices within the workforce area.

To address the third objective, we reviewed leading project monitoring practices and guidance from the Software Engineering Institute.[7] We then selected two practices[8] that, in our professional judgment, were of most significance to managing the IITT investment given the phase of the life cycle that the investment was in and the agile development methodology that the Secret Service was using for certain projects within IITT.[9] The two selected practices were:

- Monitor program performance and conduct reviews at predetermined checkpoints or milestones by, among other things, comparing actual cost, schedule, and performance data with estimates in the program plan and identifying significant deviations from established targets or thresholds for acceptable performance levels.
- Measure and monitor agile projects on velocity (i.e., number of story points completed per sprint or release), development progression

[7]Software Engineering Institute, *Agile Metrics: Progress Monitoring of Agile Contractors*, CMU/SEI-2013-TN-029 (January 2014); and *CMMI® for Acquisition, Version 1.3* (Pittsburgh, PA: November 2010).

[8]The two selected practices are a combination of multiple practices identified by the Software Engineering Institute, which we consolidated together. In particular, the first practice is a combination of four practices identified by the Institute that were associated with monitoring program performance and progress. The second practice is a combination of four agile metrics that the Institute identified as important for successful agile implementations.

[9]Agile is a type of incremental development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach.

(e.g., the number of features and user stories[10] planned and accepted), product quality (e.g., number of defects), and post-deployment user satisfaction.

To determine the extent to which DHS and the Secret Service had implemented the first selected practice, we analyzed relevant program management and governance documentation for IITT's Enabling Capabilities program, and Multi-Level Security, Uniformed Division Resource Management System, and Events Management projects.[11] For example, we analyzed documentation such as DHS and Secret Service program oversight reviews. We then assessed the documentation against the selected practice.

To determine the extent to which the Secret Service had implemented the second selected practice related to measuring and monitoring agile projects on agile metrics (i.e., velocity, development progression, product quality, and post-deployment user satisfaction), we obtained and analyzed agile-related documentation for the two projects that the Secret Service was implementing using an agile methodology—Uniformed Division Resource Management System and Events Management. Specifically, to determine the extent to which the Secret Service was measuring and monitoring these two projects on metrics for velocity and development progression, we obtained and analyzed documentation, such as sprint burndown charts and monthly program status reports, and compared it to the selected practice.

In addition, the agile metrics for product quality and post-deployment user satisfaction were only applicable to projects that had been deployed to users. As such, these metrics were applicable to the Uniformed Division Resource Management System (which the Secret Service had deployed to users) and were not applicable to Events Management (which the Secret Service had not yet deployed to users, as of early May 2018).

[10]User stories convey the customers' requirements at the smallest and most discrete unit of work that must be done to create working software. Each user story is assigned a level of effort, called story points, which is a relative unit of measure used to communicate complexity and progress between the business and development sides of the project.

[11]Uniformed Division Resource Management System and Events Management are projects within IITT's Enterprise Resource Management System program. This program also includes a third project—called Enterprise-wide Scheduling—which was still in the planning phase, as of June 2018. As such, we did not review the Enterprise-wide Scheduling project. We also did not review the Enterprise Resource Management System at the program level.

We therefore obtained and analyzed documentation demonstrating that Secret Service OCIO measured product defects for the Uniformed Division Resource Management System. We also requested documentation demonstrating that OCIO had measured and monitored post-deployment user satisfaction for this project. See appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from May 2017 to November 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Secret Service plays a critical role in protecting the President, Vice President, their immediate families, and national leaders, among others. In addition, the component is responsible for safeguarding the nation's currency and financial payment systems. To accomplish its mission, Secret Service officials reported that, as of June 2018, the component had approximately 7,100 employees (including the Uniformed Division,[12] special agents,[13] and administrative, professional, and technical staff). These employees were assigned to the component's headquarters in Washington, D.C., and 133 field offices located throughout the world (including 115 domestic offices and 18 international offices).

The Secret Service's employees are heavily dependent on the component's IT infrastructure and communications systems to perform their daily duties. According to data reported on the Office of Management and Budget's IT Dashboard,[14] the component planned to spend approximately $104.8 million in fiscal year 2018 to modernize and maintain its IT environment.

To manage this IT environment, the Secret Service hired a full-time CIO in November 2015. In addition, in an effort to improve its management structure, the component consolidated all IT staff and assets under this new CIO in March 2017. OCIO officials stated that these staff include the government employees who provide direct and indirect support of the day-to-day operations of the Secret Service's enterprise systems and services.

[12]The Uniformed Division performs duties, as prescribed by the Director of the Secret Service, in connection with the protection of certain facilities, including the White House and the Treasury Building, among others.

[13]Special agents conduct investigations to identify, locate, and apprehend criminal organizations and individuals targeting the nation's critical financial infrastructure and payment systems. Special agents also conduct protective intelligence—investigating threats against protected persons, including the President, and protected facilities, such as protectee residences.

[14]The Office of Management and Budget's IT Dashboard is a public website that provides detailed information on IT investments at 26 federal agencies.

According to Secret Service officials, the component's IT workforce included 190 staff, as of July 2018.[15] These officials stated that 166 of these employees were located in the component's headquarters in Washington, D.C., and 24 were located in domestic field offices.[16] The officials also reported that these July 2018 staffing levels were below their current approved staffing level of 220 staff (which included 44 positions in domestic field offices).

Secret Service IT staff also deploy to other locations, as necessary, to provide support for certain security activities. For example, the Secret Service reported that, in 2017, OCIO deployed over 79 staff to New York, N.Y., to provide communications support during the United Nations General Assembly.

DHS IT Acquisition Policies and Guidance

As a component of DHS, the Secret Service must follow the department's policies and processes for managing acquisitions, including IT acquisitions. DHS categorizes its acquisition programs according to three levels that are determined by the life cycle costs of the programs. These levels then determine the extent of required program and project management and the acquisition decision authority (the individual responsible for management and oversight of the acquisition). The department also categorizes its acquisition programs as major or non-major based on expected cost. Table 1 describes the levels of DHS's acquisition programs and their associated acquisition decision authorities.

Table 1: Levels of the Department of Homeland Security's (DHS) Acquisition Programs

Level	Category	Life cycle cost estimates	Acquisition decision authority
1	Major	Greater than or equal to $1 billion	DHS Under Secretary for Management/Chief Acquisition Officer
2	Major	$300 million or more, but less than $1 billion	DHS Under Secretary for Management/Chief Acquisition Officer, or the Component Acquisition Executive
3	Non-major	Less than $300 million	Component Acquisition Executive

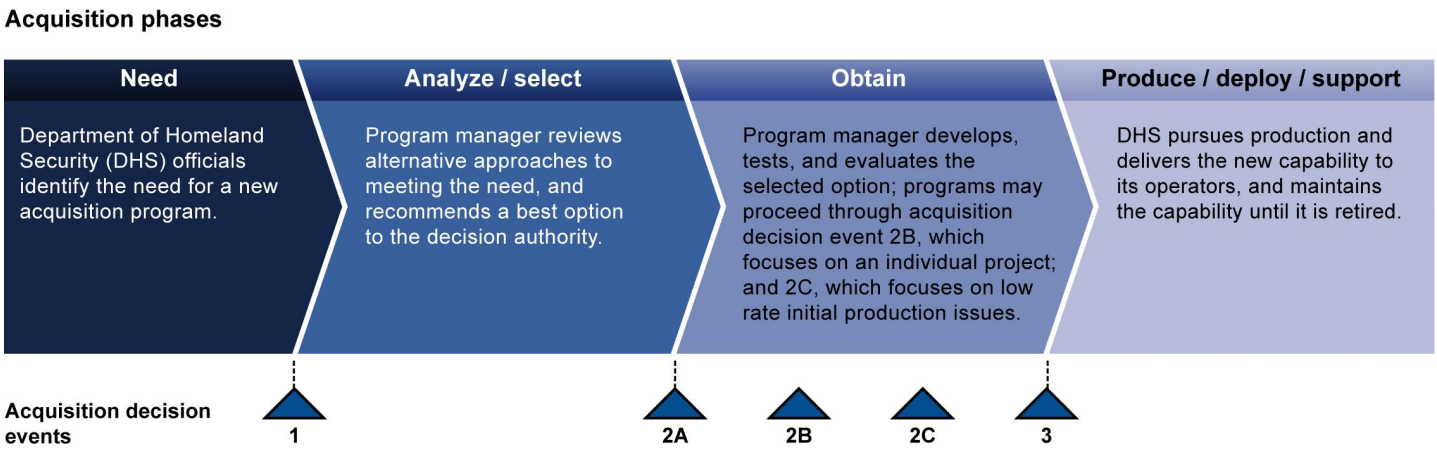
Source: GAO analysis of DHS data. | GAO-19-60.

[15]According to OCIO officials, in addition to the 190 IT support staff, the office also includes 11 special agents who assist with defining operational requirements from the field and translating them into IT requirements.

[16]As of June 2018, OCIO officials stated that no IT staff were located in the Secret Service's 18 international field offices. These officials stated that the field offices receive virtual support from IT staff in domestic offices.

DHS's policies and processes for managing major acquisition programs are primarily set forth in its Acquisition Management Directive 102-01 and Acquisition Management Instruction 102-01-001.[17] In particular, these policies establish that a major acquisition program's decision authority is to review the program at a series of predetermined acquisition decision events to assess whether the program is ready to proceed through the acquisition life cycle phases. Figure 1 depicts the acquisition life cycle established in DHS acquisition management policy.

Figure 1: Department of Homeland Security Acquisition Life Cycle for Major Acquisition Programs



Source: GAO analysis of DHS data. | GAO-19-60

DHS's Acquisition Management Directive and Instruction do not establish an acquisition life cycle framework for the department's non-major acquisition programs. Instead, according to the Instruction, Component Acquisition Executives (i.e., the senior acquisition official within a component that is responsible for implementation, management, and oversight of the component's acquisition process) are required to establish component-specific non-major acquisition policies and guidance that support the "spirit and intent" of the department's acquisition policies.

To that end, the Secret Service developed a policy that establishes an acquisition life cycle framework for its non-major acquisition programs.[18]

[17]DHS has issued multiple updates to its Acquisition Management Directive and Instruction. DHS issued the current version of the directive on July 28, 2015, and the current version of the instruction on March 9, 2016.

[18]The U.S. Secret Service, *Acquisition Management Manual*, ACQ-01 (Dec. 4, 2014).

This acquisition framework for the component's non-major acquisition programs is consistent with the acquisition framework that DHS established for its major acquisition programs. In particular, the Secret Service's framework includes the same phases and decision events as DHS's framework (e.g., acquisition decision event 2A, the point at which the acquisition decision authority determines whether a program may proceed into the obtain phase).

In addition, DHS's Systems Engineering Life Cycle Instruction and Guidebook outline a framework of major systems engineering activities and technical reviews that are to be conducted by all DHS programs and projects, both major and non-major.[19] This framework is intended to ensure that appropriate systems engineering activities are planned and implemented, and that a program's development effort is meeting the business need.

In particular, the systems engineering life cycle framework consists of nine major activities (e.g., requirements definition, integration, and testing) and a set of related technical reviews (e.g., preliminary design review) and artifacts (e.g., requirements documents). DHS policy allows programs to tailor these activities, technical reviews, and artifacts based on the unique characteristics of the program (e.g., scope, complexity, and risk). For example, a program may combine systems engineering technical reviews and artifacts, or add additional reviews. This tailored approach must be documented in a program's systems engineering life cycle tailoring plan.

The systems engineering technical reviews are intended to provide DHS the opportunity to determine how well a program has completed the necessary systems engineering activities. Each technical review includes a minimum set of exit criteria that must be satisfied before a program may move on to the next systems engineering activity. At the end of the technical review, the program manager must develop a technical review completion letter that documents the outcome of the review, including stakeholder concurrence that the exit criteria were satisfied.

Moreover, DHS's agile instruction, which was first issued in April 2016 and updated in April 2018, identifies agile as the preferred development

[19]DHS Instruction 102-01-103, *Systems Engineering Life Cycle* (November 2015) and DHS Guidebook 102-01-103-01, *Systems Engineering Life Cycle Guidebook* (April 2016).

approach for the department's IT programs and projects.[20] Agile is a type of incremental (i.e., modular) development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach.[21] DHS's agile instruction also states that component CIOs are to set modular (i.e., incremental) outcomes and target measures to monitor progress in achieving agile implementation for IT programs and projects. To that end, the department identified core metrics that its agile IT programs are to use to monitor progress, including the number of story points completed per release and the number of releases per quarter.

Further, DHS policy and guidance have established an acquisition (i.e., contract) review process that is intended to enable the DHS CIO to review and effectively guide the department's IT expenditures. According to the department's IT acquisition review guidance, DHS components with a CIO (which includes the Secret Service) are to submit to DHS OCIO for review, IT acquisitions that (1) have total estimated procurement values of $2.5 million or more; and (2) are funded by a level 1, 2, or 3 program with a life cycle cost estimate of at least $50 million (i.e., a major investment, as defined by DHS's capital planning and investment control guidance).[22]

DHS Policies Outline Component-Level CIO Responsibilities

DHS policies and guidance also establish numerous responsibilities for the department's component-level CIOs that are aimed at ensuring proper oversight and management of the components' IT investments. Among other things, these component-level CIO responsibilities relate to topics such as IT budgeting, portfolio management, and oversight of programs' systems engineering life cycles. Table 2 identifies 14 selected IT oversight responsibilities for DHS's component CIOs.

[20]DHS Instruction 102-01-004, *Agile Development and Delivery for Information Technology* (April 2018).

[21]A traditional waterfall software development effort is usually a broadly scoped, multiyear effort that produces a product at the end of a long sequence of phases.

[22]DHS's threshold for a major investment (a life cycle cost estimate of at least $50 million) is different than the department's threshold for major acquisition programs. As discussed earlier, DHS's acquisition management guidance defines major acquisitions as those with life cycle cost estimates of at least $300 million.

Table 2: Selected Component-Level Chief Information Officer (CIO) Responsibilities Outlined in Department of Homeland Security (DHS) Policies and Guidance

DHS component-level CIO responsibility	DHS policy outlining responsibility
1. Develop and review the component information technology (IT) budget formulation and execution.	Directive 142-02, *IT Integration and Management* (February 2014)[a]
2. Manage the component IT investment portfolio, including establishing an IT acquisition review process that enables component and DHS review of component acquisitions (i.e., contracts) that contain IT.	Directive 102-02, *Capital Planning and Investment Control* (February 2016) and Instruction 102-02-001, *Capital Planning and Investment Control Guidebook* (March 2016)
3. Develop, implement, and maintain a detailed IT strategic plan.	Directive 142-02
4. Ensure all component IT policies are in compliance and alignment with DHS IT directives and instructions.	Directive 142-02
5. Concur with each program's and/or project's systems engineering life cycle tailoring plan.	Instruction 102-01-103, *Systems Engineering Life Cycle* (November 2015)
6. Support the Component Acquisition Executive to ensure processes are established that enable systems engineering life cycle technical reviews and that they are adhered to by programs and/or projects.	Instruction 102-01-103
7. Ensure that all systems engineering life cycle technical review exit criteria are satisfied for each of the component's IT programs and/or projects.	Instruction 102-01-103
8. Ensure the necessary systems engineering life cycle activities have been satisfactorily completed as planned for each of the component's IT programs and/or projects.	Instruction 102-01-103
9. Concur with the systems engineering life cycle technical review completion letter for each of the component's IT programs and/or projects.	Instruction 102-01-103
10. Maintain oversight of the component's agile development approach[b] for IT by appointing the responsible personnel, identifying investments for adoption, and reviewing artifacts.	Instruction 102-01-004, *Agile Development and Delivery for IT* (April 2016)
11. With Component Acquisition Executives, evaluate and approve the application of agile development for IT programs consistent with the component's agile development approach.	Instruction 102-01-004
12. Set modular outcomes and target measures to monitor progress in achieving agile implementation for IT programs and/or projects within the component.	Instruction 102-01-004
13. Participate on DHS's CIO Council,[c] Enterprise Architecture Board,[d] or other councils/boards as appropriate, and appoint employees to serve, when necessary.	Directive 142-02
14. Meet the IT competency requirements established by the DHS CIO, as required in the component CIO's performance plan.	Directive 142-02

Source: GAO analysis of DHS policies and guidance. | GAO-19-60.

[a]DHS issued an updated version of this policy in April 2018, near the end of our review. The updated policy includes minor revisions and clarifications that do not change the intent of our selected responsibilities.

[b]Agile is a type of incremental development that calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach that produces a product at the end of the sequence.

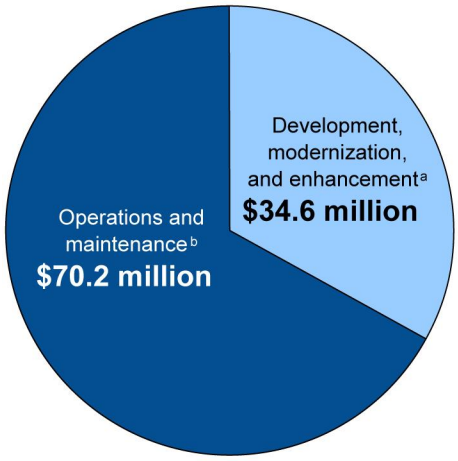
[c]DHS's CIO Council is responsible for setting the vision and strategy for the IT function and information resources within DHS, and for leading the delivery of IT-enabled mission capabilities in a timely and effective manner.

[d]DHS's Enterprise Architecture Board is responsible for evaluating and approving IT investments for alignment with the enterprise architecture and for ensuring that the architecture is updated and maintained.

Overview of the Secret Service's IT Portfolio

The Secret Service acquires IT infrastructure and services that are intended to improve its ability to execute its investigation and protection missions. According to data reported on the Office of Management and Budget's IT Dashboard, the Secret Service planned to spend about $104.8 million on IT in fiscal year 2018, which included approximately $34.6 million for the development and modernization of its IT infrastructure and services, and about $70.2 million for the operations and maintenance of this infrastructure (including 21 existing IT systems). Also according to data reported on the IT Dashboard, as of April 2018, the Secret Service had one major IT investment (called the Information Integration and Technology Transformation and discussed in more detail later in this report), seven non-major IT investments, and one non-standard infrastructure investment.[23] Figure 2 depicts the Secret Service's planned IT spending for fiscal year 2018.

Figure 2: The U.S. Secret Service's Planned Information Technology (IT) Spending for Fiscal Year 2018



Source: GAO analysis of the Secret Service's planned IT spending data reported on the Office of Management and Budget's IT Dashboard. | GAO-19-60

[a]According to the Office of Management and Budget, development, modernization, and enhancement refers to projects and activities leading to new IT assets and systems, as well as projects and

[23]The Office of Management and Budget requires agencies to separately classify IT infrastructure investments from major and non-major IT investments. According to the office's fiscal year 2019 IT Budget – Capital Planning Guidance, non-standard infrastructure investments for fiscal year 2019 can include all costs except for IT security and compliance, and IT management costs.

activities that change or modify existing IT assets to: substantively improve capability or performance, implement legislative or regulatory requirements, or meet an agency leadership request.

[b]According to the Office of Management and Budget, operations and maintenance costs refer to the expenses required to operate and maintain an IT asset that is operating in a production environment.

The Secret Service Initiated the Information Integration and Technology Transformation Investment to Address IT Challenges

The Secret Service has faced long-standing challenges in managing its IT infrastructure. For example,

- A National Security Agency audit of the Secret Service's IT environment in 2008 identified network and system vulnerabilities that needed immediate remediation to protect the component's systems and electronic information.
- The Secret Service determined in 2010 that it had IT capability gaps associated with three key areas: network security, information sharing and situational awareness, and operational communications. The component reported that it required a significant IT modernization effort with sustained investment of resources to replace dated and restrictive network and communications capabilities.
- The Secret Service also reported in 2010 that it had 42 mission-support applications that were operating on a 1980's mainframe that lacked multi-level security (i.e., the ability to view classified information from two security levels, such as secret and top secret, at the same time), was beyond its equipment life cycle, and was at risk of failing.
- Further, in 2011, DHS's Office of Inspector General reported that the Secret Service's existing infrastructure did not meet current operational requirements.[24] According to the Secret Service, this dated infrastructure was unable to support newer technologies (e.g., Internet protocol[25]), share common DHS enterprise services, or migrate to the department's consolidated data centers.

[24]DHS Office of Inspector General, *U.S. Secret Service's Information Technology Modernization Effort*, OIG-11-56 (March 2011).

[25]Internet protocol is one of the primary mechanisms that define how and where information such as text, voice, and video moves across interconnected networks.

To address challenges with its IT environment, in 2009, the Secret Service initiated the IITT investment, which is intended to modernize and enhance the component's infrastructure, communications systems, applications, and processes. In particular, IITT is a portfolio of programs and projects that are meant to, among other things, improve systems availability in support of the Secret Service's business operations, increase interoperability with other government systems and networks, enhance the component's system and network security, and enable scalability to support growth.

From 2010 to July 2018, according to OCIO officials, the Secret Service spent approximately $392 million on IITT. In fiscal year 2018, the component had planned to spend approximately $42.7 million on IITT (i.e., about 40 percent of its total planned IT spending for the fiscal year), according to data reported on the Office of Management and Budget's IT Dashboard. In total, the planned life cycle cost estimate for IITT is at least $811 million.[26]

As of June 2018, IITT was a major investment comprised of two programs (one of which included three projects) and one standalone project (i.e., it was not part of another program) that had capabilities that were in planning or development and modernization. These programs and project were the Enabling Capabilities program, Enterprise Resource Management System program (which included three projects that were each being implemented using an agile methodology:[27] Uniformed Division Resource Management System, Events Management, and Enterprise-wide Scheduling), and the Multi-Level Security project.

[26]Secret Service OCIO officials were unable to provide a complete life cycle cost estimate for the investment. According to the officials, DHS requires such estimates for acquisition programs and projects, but IITT is considered a "Program, Project, and Activity" that includes a portfolio of IT projects. As such, the Secret Service developed life cycle cost estimates for IITT's individual programs and projects, such as Enabling Capabilities. Given this, we compiled the Secret Service's latest planned life cycle cost estimates for IITT's programs and projects that had capabilities in planning or development and modernization, as of June 2018. We also included costs through September 2018 that the component planned to spend on other capabilities that were implemented as part of IITT and are now in operations and maintenance (as discussed later), such as communications interoperability. However, the costs for these other capabilities in operations and maintenance are not life cycle costs. As such, our estimate may not be complete.

[27]As discussed earlier, agile is a type of incremental development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach.

Table 3 describes the IITT programs and projects that had capabilities that were in planning or development and modernization, as of June 2018. The table also includes the associated level, acquisition decision authority, estimated life cycle costs, and planned or actual dates of operational capability for each of the programs and projects. (Appendix II also provides additional information on these programs and projects.)

Table 3: The U.S. Secret Service's Information Integration and Technology Transformation (IITT) Investment's Programs and Projects with Capabilities in Planning or Development and Modernization, as of June 2018

IITT program/project name and description	Level	Acquisition decision authority	Life cycle cost estimate (then-year $ in millions)	Planned or actual date of initial operational capability[a]	Planned or actual date of full operational capability[b]
Enabling Capabilities program Intended to, among other things, (1) modernize and enhance the Secret Service's information technology (IT) network infrastructure, including improving the speed and reliability of the Secret Service's IT system performance; (2) enhance cybersecurity to protect against potential intrusions and viruses; and (3) provide counterintelligence and data mining capabilities to improve officials' ability to perform the Secret Service's investigative mission.	2 (major)	Department of Homeland Security Under Secretary for Management	$622.5	April 2017[c]	June 2018[c]
Enterprise Resource Management System program This program is made up of three projects: the Uniformed Division Resource Management System, Events Management, and Enterprise-wide Scheduling.	3 (non-major)	The Secret Service Component Acquisition Executive	67.8[d]		
Uniformed Division Resource Management System project Intended to provide a system that will enable the Secret Service's Uniformed Division[e] to efficiently and effectively plan, provision, and schedule its work days.	3 (non-major)	The Secret Service Component Acquisition Executive	12.9	December 2016[c]	May 2017[c,f]
Events Management project Intended to provide a system that will unify the logistical actions (e.g., assigning personnel) surrounding special events that Secret Service agents need to protect, such as the United Nations General Assembly.	3 (non-major)	The Secret Service Component Acquisition Executive	24.3	May 2018[c]	1st quarter FY 2020
Enterprise-wide Scheduling project Intended to provide a capability for creating schedules for Secret Service agents and administrative, professional, and technical staff, as well as the ability to generate reports on information such as monthly hours worked.	3 (non-major)	The Secret Service Component Acquisition Executive	8.6	2nd quarter FY 2020	1st quarter FY 2021
Multi-Level Security project Intended to enable authorized Secret Service users to view two levels of classified information on a single workstation. Previously, data at various security levels were contained and used in multiple disparate systems. Multi-Level Security is intended to streamline users' access to information at different security levels, in order to enable them to more quickly and effectively perform their duties.	3 (non-major)	The Secret Service Component Acquisition Executive	39.8	December 2013[c]	4th quarter FY 2019

Legend: FY = fiscal year

Source: GAO analysis of U.S. Secret Service documentation and data provided by U.S. Secret Service officials. | GAO-19-60.

[a]Initial operational capability is the point at which a subset of capabilities are first fielded to select users.

[b]Full operational capability is the point at which an investment becomes fully operational.

[c]This is an actual date.

[d]Enterprise Resource Management System's total costs include approximately $22 million in sunk costs from 2009 through 2015, which were spent on the Combined Operations Logistics Database 2 program—the predecessor to the Enterprise Resource Management System. In particular, that program experienced two schedule breaches and, in 2015, based on the program's contractor making insufficient progress in developing the system, the Secret Service chose not to continue the contract.

[e]The Secret Service's Uniformed Division is to perform duties, as prescribed by the Director of the Secret Service, in connection with the protection of certain facilities, including the White House and the Treasury Building, among others.

[f]Secret Service OCIO officials stated that they completed deployment of the Uniformed Division Resource Management System to all planned users in February 2018. As such, this project was in full operations and maintenance as of February 2018.

The Enabling Capabilities program within IITT is designated as a major acquisition program. As such, its acquisition decision authority is the DHS Under Secretary for Management, and both DHS and the Secret Service provide oversight to this program. IITT's other program and project—the Enterprise Resource Management System program (which includes three projects, as discussed earlier) and Multi-Level Security project—are designated non-major acquisition programs. In June 2011, DHS's Under Secretary for Management delegated acquisition decision authority for this non-major program and project to the Secret Service Component Acquisition Executive. As such, oversight of the Enterprise Resource Management System program (including its three projects) and the Multi-Level Security project is conducted primarily at the component level.

The Secret Service also implemented other capabilities that are now in operations and maintenance (i.e., the capabilities have been fielded and are operational) as part of the IITT investment, such as a capability to move data between systems in separate classification levels (e.g., top secret and secret) and communications interoperability. Table 4 describes IITT capabilities that are in operations and maintenance.

Table 4: The U.S. Secret Service's Information Integration and Technology Transformation Investment's Capabilities That Are in Operations and Maintenance

Capability name	Description	Date of full operational capability	Planned costs through September 2018[a] ($ in millions)	Annual costs to maintain ($ in millions)
Cross Domain	A transfer capability that allows Secret Service analysts or other designated personnel to move data between systems in separate classification levels (e.g., top secret and secret).	December 2015	$3.8	$0.6
Protective Threat Management System	A case management system that is used to record information on individuals expressing threatening or inappropriate behavior, and on other incidents that may impact the Secret Service's mission to protect people, events, and facilities.	June 2012	9.3	1.3
White House Communications Agency[b] Interoperability	Hardware and software to support wireless devices to ensure reliable and consistent wireless voice, data, and radio coverage to Secret Service agents throughout the world and to allow communications interoperability between the Secret Service and the White House Communications Agency.	June 2012[c]	68.1	4.5

Source: GAO analysis of U.S. Secret Service documentation and data provided by U.S. Secret Service officials. | GAO-19-60.

[a]These costs include both the prior costs spent, as well as the approved, budgeted costs through September 30, 2018.

[b]The White House Communications Agency is a unit within the Defense Information Systems Agency. It provides information services and communications support to the President and his staff.

[c]According to Secret Service officials, this is the approximate date that the component initially achieved full interoperability with the White House Communications Agency. These officials stated that this capability was not an acquisition program; instead, it was a series of annual procurements of communications equipment and sustainment costs to establish and maintain compatibility with the White House Communications Agency. As such, it did not have a full operational capability milestone.

DHS's Management of Human Capital Is a High-Risk Effort

DHS, including the Secret Service, has faced long-standing challenges in effectively managing its workforce. In January 2003, we designated the implementation and transformation of DHS as high risk, including its management of human capital, because it had to transform 22 agencies—several with major management challenges—into one department. This represented an enormous and complex undertaking that would require time to achieve in an effective and efficient manner. Since that time, the department has made important progress in strengthening and integrating its management functions.

Nevertheless, we have continued to report that significant work remains for DHS to improve these management functions.[28] Among other things, we previously reported that the department had lower average employee morale than the average for the rest of the federal government.[29] We also reported that, in 2011, based on employee responses to the Office of Personnel Management's Federal Employee Viewpoint Survey—a tool that measures employees' perceptions of whether and to what extent conditions characterizing successful organizations are present in their agency—DHS was ranked 31st out of 33 large agencies on the Partnership for Public Service's *Best Places to Work in the Federal Government* rankings.[30] The most recent results of these surveys in 2017 showed that DHS continues to maintain its low rankings.

DHS's Office of Inspector General has reported on challenges that the Secret Service has faced in managing its IT workforce. Specifically, in October 2016, the Inspector General reported that

[28]See, for example, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[29]GAO, *Department of Homeland Security: DHS's Efforts to Improve Employee Morale and Fill Senior Leadership Vacancies*, GAO-14-228T (Washington, D.C.: Dec. 12, 2013); *Department of Homeland Security: Preliminary Observations on DHS's Efforts to Improve Employee Morale*, GAO-12-509T (Washington, D.C.: Mar. 22, 2012); and GAO-12-940.

[30]According to the Partnership for Public Service, the *Best Places to Work in the Federal Government* ranking is based on employee responses to surveys with questions related to, among other things, overall employee engagement, leadership, strategic management, innovation, and work–life balance.

- the Secret Service CIO did not have oversight of, or authority over, all IT resources, including the workforce; in particular, almost all of the component's IT employees were located in a division outside of OCIO; and
- the Secret Service had vacancies in key positions responsible for managing IT, including not having a full-time CIO from December 2014 through November 2015.[31]

As previously discussed, the Secret Service has taken actions to address these two issues with the management of its IT workforce. These actions included hiring its full-time CIO in November 2015 and consolidating the workforce and all IT assets under this CIO in March 2017.

The Secret Service CIO Fully Implemented Most of the Required Responsibilities

Of the 14 selected responsibilities established for component-level CIOs in DHS's IT management policies, the Secret Service CIO had fully implemented 11 responsibilities and had partially implemented 3 responsibilities. Table 5 summarizes the extent to which the Secret Service CIO had implemented each of the 14 responsibilities.

[31]DHS Office of Inspector General, *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01 (Washington, D.C.: Oct. 7, 2016).

Table 5: Summary of the U.S. Secret Service Chief Information Officer's (CIO) Implementation of 14 Selected Component-Level CIO Responsibilities Outlined in Department of Homeland Security (DHS) Policies

DHS component-level CIO responsibility	Fully implemented	Partially implemented
1. Develop and review the component information technology (IT) budget formulation and execution.	Yes	No
2. Manage the component IT investment portfolio, including establishing an IT acquisition review process that enables component and DHS review of component acquisitions (i.e., contracts) that contain IT.	No	Yes
3. Develop, implement, and maintain a detailed IT strategic plan.	Yes	No
4. Ensure all component IT policies are in compliance and alignment with DHS IT directives and instructions.	No	Yes
5. Concur with each program's and/or project's systems engineering life cycle tailoring plan.[a]	Yes	No
6. Support the Component Acquisition Executive to ensure processes are established that enable systems engineering life cycle technical reviews and that they are adhered to by programs and/or projects.	Yes	No
7. Ensure that all systems engineering life cycle technical review exit criteria are satisfied for each of the component's IT programs and/or projects.	Yes	No
8. Ensure the necessary systems engineering life cycle activities have been satisfactorily completed as planned for each of the component's IT programs and/or projects.	Yes	No
9. Concur with the systems engineering life cycle technical review completion letter for each of the component's IT programs and/or projects.	Yes	No
10. Maintain oversight of their component's agile development approach[b] for IT by appointing the responsible personnel, identifying investments for adoption, and reviewing artifacts.	Yes	No
11. With Component Acquisition Executives, evaluate and approve the application of agile development for IT programs consistent with the component's agile development approach.	Yes	No
12. Set modular outcomes and target measures to monitor the progress in achieving agile implementation for IT programs and/or projects within their component.	No	Yes
13. Participate on DHS's CIO Council,[c] Enterprise Architecture Board,[d] or other councils/boards as appropriate, and appoint employees to serve when necessary.	Yes	No
14. Meet the IT competency requirements established by the DHS CIO, as required in the component CIO's performance plan.	Yes	No
Total	**11**	**3**

Source: GAO analysis of data provided by U.S. Secret Service and DHS officials. | GAO-19-60.

[a]DHS's systems engineering life cycle framework consists of nine major activities and a set of related technical reviews (e.g., preliminary design review) and artifacts (e.g., requirements documents). DHS policy allows programs to tailor these activities, technical reviews, and artifacts based on the unique characteristics of the program (e.g., scope, complexity, and risk). This tailored approach must be documented in a program's systems engineering life cycle tailoring plan.

[b]Agile is a type of incremental development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach.

[c]DHS's CIO Council is responsible for setting the vision and strategy for the IT function and information resources within DHS, and for leading the delivery of IT-enabled mission capabilities in a timely and effective manner.

[d]DHS's Enterprise Architecture Board is responsible for evaluating and approving IT investments for alignment with the enterprise architecture and for ensuring that the architecture is updated and maintained.

The Secret Service CIO fully implemented 11 of the 14 selected component-level CIO responsibilities. Examples of the responsibilities that the CIO fully implemented are as follows:

- **Develop, implement, and maintain a detailed IT strategic plan.** Consistent with DHS's IT Integration and Management directive, in January 2017, the Secret Service CIO developed an IT strategic plan that outlined the CIO's strategic IT goals and objectives, as well as tasks intended to meet the goals and objectives. The CIO maintained this strategic plan, to include updating it in January 2018. The CIO also took steps to implement the tasks identified within the strategic plan, such as working to develop an IT training program. In particular, as part of this effort to develop an IT training program, OCIO identified recommended training for the office's various IT workforce groups (discussed in more detail later in this report).

- **Concur with each program's and/or project's systems engineering life cycle tailoring plan.**[32] In accordance with DHS's Systems Engineering Life Cycle instruction, the Secret Service CIO concurred with the systems engineering life cycle tailoring plan for one program and three projects included in the Secret Service's IITT investment. Specifically, the CIO documented his approval via his signature on the tailoring plans for IITT's Enabling Capabilities program, and Multi-Level Security, Uniformed Division Resource Management System, and Events Management projects.

- **Participate on DHS's CIO Council, Enterprise Architecture Board, or other councils/boards as appropriate, and appoint employees to serve when necessary.**[33] As required by DHS's IT Integration and

[32]As previously discussed, DHS's systems engineering life cycle framework consists of nine major activities and a set of related technical reviews (e.g., preliminary design review) and artifacts (e.g., requirements documents). DHS policy allows programs to tailor these activities, technical reviews, and artifacts based on the unique characteristics of the program (e.g., scope, complexity, and risk). This tailored approach must be documented in a program's systems engineering life cycle tailoring plan.

[33]DHS's CIO Council is responsible for setting the vision and strategy for the IT function and information resources within the department, as well as for leading the delivery of IT-enabled mission capabilities in a timely and effective manner. In addition, DHS's Enterprise Architecture Board is responsible for evaluating and approving IT investments for alignment with the enterprise architecture and for ensuring that the architecture is updated and maintained. According to a DHS OCIO program management specialist, there are no other boards or councils on which the Secret Service CIO is required to participate.

Management directive, the Secret Service CIO participated on two required DHS-level councils/boards, and appointed a delegate to serve in his place, when necessary. Specifically, the Secret Service CIO or the CIO's delegate—the Deputy CIO—attended bi-monthly meetings of the DHS CIO Council. In addition, another Secret Service CIO appointee—the component's Chief Architect—attended an ad hoc meeting of the Enterprise Architecture Board in June 2017.[34]

In addition, the Secret Service CIO had partially implemented three component-level CIO responsibilities, as follows.

- **Manage the component IT investment portfolio, including establishing a component-level IT acquisition review process that enables component and DHS review of component acquisitions (i.e., contracts) that contain IT.** As directed in DHS's Capital Planning and Investment Control directive and guidebook, the Secret Service CIO took steps to manage the component's IT investment portfolio, including reviewing certain contracts containing IT. For example, among our random sample of 33 IT contracts that the Secret Service awarded between October 1, 2016, and June 30, 2017, we found that the CIO or the CIO's delegate had reviewed 31 of these contracts.

  However, the CIO had not established and documented a defined process for reviewing contracts containing IT, which may have contributed to why the CIO or the CIO's delegate did not review 2 of the 33 contracts in our sample. OCIO officials were unable to explain why neither of these officials reviewed the 2 contracts, which had a combined planned total procurement value of approximately $1.75 million. In particular, one of the contracts, with a planned total procurement value of about $1,122,934, was to provide credentialing services for the 2017 Presidential Inauguration. The other contract, with a planned total procurement value of about $629,337, was to provide maintenance support for a logistics system. The OCIO officials acknowledged that both contracts should have been approved by one of these officials. Without establishing and documenting an IT acquisition review process that ensures that the CIO or the CIO's delegate reviews all contracts containing IT, as

[34]According to DHS OCIO officials in June 2018, the department's Enterprise Architecture Board meets on an ad hoc basis to review issues of enterprise-wide significance or component programs of particular interest to DHS leadership.

appropriate, the CIO's ability to analyze the contracts to ensure that they are a cost-effective use of resources and are aligned with the component's missions and goals is limited.

- **Ensure all component IT policies are in compliance and alignment with DHS IT directives and instructions.** As required by DHS's IT Integration and Management directive, the Secret Service CIO had ensured that certain component IT policies were in compliance and alignment with DHS IT directives and instructions. For example, in alignment with the department's IT Integration and Management directive, the Secret Service's Investment Governance for IT policy specifies that the component CIO (in conjunction with each Secret Service Office) is responsible for developing the component IT spend plan, as well as developing and maintaining an IT strategic plan.

  However, the Secret Service's enterprise governance policy was not in compliance with DHS's IT Integration and Management directive. Specifically, while the department's policy states that the Secret Service CIO is responsible for developing and reviewing the component's IT budget formulation and execution, the Secret Service's enterprise governance policy does not specify this as the CIO's responsibility.

  According to OCIO officials, the Secret Service CIO participates in the development and review of the IT budget formulation and execution as a member of the Executive Resources Board (the Secret Service's highest-level governing body, which has the final decision authority and responsibility for enterprise governance), and the Secret Service Deputy CIO is a voting member of the Enterprise Governance Council (the Secret Service's second-level governance body and advisory council to the Executive Resources Board). However, the Secret Service's enterprise governance policy has not been updated to reflect these roles. The Secret Service did not update its enterprise governance policy to properly reflect the CIO's and Deputy CIO's roles on the Executive Resources Board or Enterprise Governance Council because OCIO officials were not aware that these roles were not properly documented in the component's policy until we identified this issue during our review.

  Further compounding the issue of the Secret Service's enterprise governance policy not properly reflecting the CIO's and Deputy CIO's roles and responsibilities on the component's governance boards is

that the Secret Service has not developed a charter for its Executive Resources Board. We have previously reported that a best practice for effective investment management is to define and document the board's membership, roles, and responsibilities.[35] One such way to do so is via a charter.

According to Secret Service officials, the component does not have a charter for the board because, while the Secret Service has established the board pursuant to law, there is little statutory guidance on how the board must be formalized, including whether a charter is required. The officials acknowledged that development of a board charter is a best practice. They stated that, in response to our review, the component has begun efforts to develop a charter for the Executive Resources Board, but they did not know when it would be completed.

Until the Secret Service updates its enterprise governance policy to specify (1) the CIO's current role and responsibilities on the Executive Resources Board, to include developing and reviewing the IT budget formulation and execution, and (2) the Deputy CIO's role and responsibilities on the Enterprise Governance Council, the CIO's ability to develop and review the component's IT budget may be limited. Further, until the Secret Service develops a charter for its Executive Resources Board that specifies the roles and responsibilities of all board members, including the CIO, the Secret Service will not be effectively positioned to ensure that all members understand their roles and responsibilities on the board and will perform them as expected.

- **Set modular outcomes and target measures to monitor the progress in achieving agile implementation for IT programs and/or projects within their component.** Consistent with DHS policy, the Secret Service CIO has set modular outcomes and target measures to monitor the progress of two IITT projects that the component is implementing using an agile methodology—Uniformed

[35]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23)*, GAO-04-394G (Washington, D.C.: Mar. 1, 2004).

Division Resource Management System and Events Management.[36] For example, the modular outcomes set for these projects included measuring planned and actual burndown (i.e., the number of user stories[37] completed). In addition, the projects were to measure their velocity (i.e., the rate of work completed) for each sprint (i.e., a set period of time during which the development team is expected to complete tasks related to developing a piece of working software).

However, the modular outcomes and target measures did not include product quality or post-deployment user satisfaction, although such measures are leading practices for managing agile projects.[38] According to Secret Service OCIO officials, the component does not mandate the specific metrics that its agile projects are to use; instead, each project is to determine the metrics based on stakeholder requirements and unique project characteristics. The officials further stated that these metrics are to be documented in an acquisition program baseline and program management plan; this baseline and program management plan are then to be approved by the CIO. To its credit, the component's one agile project that, as of May 2018, had deployed its system to users—the Uniformed Division Resource Management System—did measure product quality. OCIO officials also stated that they regularly receive verbal, undocumented feedback from users on the system and they plan to conduct a documented user satisfaction survey on this system by September 2018.

Nevertheless, without ensuring that product quality and post-deployment user satisfaction metrics are included in the modular outcomes and target measures that the CIO sets for monitoring agile projects, the Secret Service lacks assurance that the Events Management project or other future agile projects will measure product quality or post-deployment user satisfaction. Without guidance specifying that agile projects track these metrics, the

[36]The Secret Service also had a third project—called Enterprise-wide Scheduling—on which the component planned to use agile; however, as of June 2018, the Secret Service had not yet begun development on this project.

[37]User stories convey the customers' requirements at the smallest and most discrete unit of work that must be done to create working software. Each user story is assigned a level of effort, called story points, which is a relative unit of measure used to communicate complexity and progress between the business and development sides of the project.

[38]Software Engineering Institute, *Agile Metrics: Progress Monitoring of Agile Contractors*, CMU/SEI-2013-TN-029 (January 2014).

projects may not do so and the CIO may be limited in his knowledge of the progress being made on these projects.

The Secret Service Did Not Fully Implement the Majority of the Selected Leading Planning and Management Practices for Its IT Workforce

Workforce planning and management is essential for ensuring that federal agencies have the talent, skill, and experience mix they need to execute their missions and program goals. To help agencies effectively conduct workforce planning and management, the Office of Personnel Management, the Chief Human Capital Officers Council, DHS, the Secret Service, and we have identified numerous leading practices related to five workforce areas: strategic planning, recruitment and hiring, training and development, employee morale, and performance management.[39] Table 6 identifies the five workforce areas and 15 selected leading practices associated with these areas (3 practices within each area).

[39]Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative* (Sept. 2008); DHS, Instruction 102-01-001*, Acquisition Management Instruction* (Mar. 9, 2016); the U.S. Secret Service, *Acquisition Workforce Certification*, ADM-10 (04) (Dec. 19, 2012); GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016); *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans*, GAO-12-940 (Washington, D.C.: Sept. 28, 2012); *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 1, 2004); and *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*, GAO-03-488 (Washington, D.C., Mar. 14, 2003).

Table 6: Selected Workforce Planning and Management Areas and Selected Leading Practices Associated with Each Area

Workforce area	Leading practice
1. Strategic planning	1. Establish and maintain a strategic workforce planning process, including developing all competency and staffing needs.
	2. Regularly assess competency and staffing needs, and analyze the IT workforce to identify gaps in those areas.
	3. Develop strategies and plans to address gaps in competencies and staffing.
2. Recruitment and hiring	4. Implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process.
	5. Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps.
	6. Adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics.
3. Training and development	7. Establish a training and development program to assist the agency in achieving its mission and goals.
	8. Use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable.
	9. Collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.
4. Employee morale	10. Determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans. Develop and implement action plans to improve employee morale.
	11. Establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale.
	12. Maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale.
5. Performance management	13. Establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance.
	14. Explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals.
	15. Periodically provide individuals with regular performance feedback.

Source: GAO analysis of workforce-related areas and practices identified in federal and agency guidance, and GAO's prior work. | GAO-19-60.

Of the five selected workforce planning and management areas, the Secret Service had substantially implemented two of the areas and minimally implemented three of the areas for its IT workforce. In addition, of the 15 selected leading practices associated with these workforce planning and management areas, the Secret Service had fully implemented 3 practices, partly implemented 8 practices, and did not implement any aspects of 4 practices. Table 7 summarizes the extent to which the Secret Service had implemented for its IT workforce the five

selected workforce planning and management areas and 15 selected leading practices associated with those areas, as of June 2018.

Table 7: The U.S. Secret Service's Implementation of Five Selected Workforce Planning and Management Areas and 15 Selected Associated Leading Practices for Its Information Technology (IT) Workforce, as of June 2018

Workforce area	Overall area rating[a]	Practice rating	Leading practice
Strategic planning	Minimally implemented	Partly implemented	1. Establish and maintain a strategic workforce planning process, including developing all competency and staffing needs.
		Not implemented	2. Regularly assess competency and staffing needs, and analyze the IT workforce to identify gaps in those areas.
		Partly implemented	3. Develop strategies and plans to address gaps in competencies and staffing.
Recruitment and hiring	Minimally implemented	Partly implemented	4. Implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process.
		Not implemented	5. Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps.
		Not implemented	6. Adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics.
Training and development	Minimally implemented	Partly implemented	7. Establish a training and development program to assist the agency in achieving its mission and goals.
		Partly implemented	8. Use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable.
		Not implemented	9. Collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.
Employee morale	Substantially implemented[b]	Fully implemented	10. Determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans. Develop and implement action plans to improve employee morale.
		Fully implemented	11. Establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale.
		Partly implemented	12. Maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale.
Performance management	Substantially implemented	Partly implemented	13. Establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance.
		Partly implemented	14. Explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals.
		Fully implemented	15. Periodically provide individuals with regular performance feedback.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

[a]Our methodology includes five levels of workforce area ratings based on the implementation of the three selected leading practices within each area:

- *Fully implemented:* The Secret Service provided evidence that it had fully implemented all three of the selected practices within the workforce area.
- *Substantially implemented:* The Secret Service provided evidence that it had either
  - fully implemented one selected practice and partly implemented the remaining two selected practices within the workforce area, or
  - fully implemented two selected practices and partly implemented the remaining one selected practice within the workforce area.
- *Partially implemented:* The Secret Service provided evidence that it had partly implemented each of the three selected practices within the workforce area.
- *Minimally implemented:* The Secret Service provided evidence that it had either
  - partly implemented one selected practice and did not implement the remaining two selected practices within the workforce area, or
  - partly implemented two selected practices and did not implement the remaining one selected practice within the workforce area.
- *Not implemented:* The Secret Service did not provide evidence that it had implemented any of the three selected practices within the workforce area.

[b]While the Secret Service substantially implemented the selected employee morale practices for its IT workforce and the majority of the component's IT staff reported that their morale was "very good" or "excellent" as of December 2017, additional work remains for the Secret Service and the Department of Homeland Security to improve employee morale across the Secret Service and the department. We have ongoing work to monitor the department's efforts to address this high-risk issue.

The Secret Service Minimally Implemented Selected Leading IT Strategic Workforce Planning Practices

Strategic workforce planning is an essential activity that an agency needs to conduct to ensure that its human capital program aligns with its current and emerging mission and programmatic goals, and that the agency is able to meet its future needs. We previously identified numerous leading practices related to IT strategic workforce planning, including that an organization should (1) establish and maintain a strategic workforce planning process, including developing all competency and staffing needs; (2) regularly assess competency and staffing needs, and analyze the IT workforce to identify gaps in those areas; and (3) develop strategies and plans to address gaps in competencies and staffing.[40]

The Secret Service minimally implemented the three selected leading practices associated with the IT strategic workforce planning area. Specifically, the component partly implemented two of the practices and did not implement one practice. Table 8 lists these selected leading

[40]GAO-17-8.

practices and provides our assessment of the Secret Service's implementation of the practices.

Table 8: The U.S. Secret Service's Implementation of Selected Leading IT Strategic Workforce Planning Practices, as of June 2018

Overall workforce area rating	Practice rating	Leading practice
Minimally implemented	Partly implemented	1. Establish and maintain a strategic workforce planning process, including developing all competency and staffing needs.
	Not implemented	2. Regularly assess competency and staffing needs, and analyze the IT workforce to identify gaps in those areas.
	Partly implemented	3. Develop strategies and plans to address gaps in competencies and staffing.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

- **Establish and maintain a strategic workforce planning process, including developing all competency and staffing needs—partly implemented.** The Secret Service took steps to establish a strategic workforce planning process for its IT workforce. For example, the Secret Service CIO developed and maintained a plan that identified strategic workforce planning tasks, to include analyzing the staffing requirements of the IT workforce. In addition, the Secret Service defined general core competencies (e.g., communication and customer service) for its workforce, including IT staff.

  However, OCIO did not identify all required knowledge and skills needed to support this office's functions. In particular, while OCIO identified certain technical competencies that its IT workforce needs, such as cybersecurity, the office did not identify and document all of the technical competencies that it needs. OCIO officials stated that they did not identify and document the technical competencies that the office needs because the Secret Service was focused on reorganizing the IT workforce under a single, centralized reporting chain within the CIO's office. Consequently, the officials stated that they had not completed the work to identify all required IT knowledge and skills necessary to support the office.

  Yet, the Secret Service completed the IT workforce reorganization effort over a year ago, in March 2017 and, since then, OCIO has not identified all of the required IT knowledge and skills that the office needs. OCIO officials told us that they plan to identify all of the technical competency needs for the IT workforce, but they were unable to specify a time frame for when these needs would be fully

identified. Until OCIO identifies all of the required knowledge and skills for the IT workforce, the office will be limited in its ability to identify and address any competency gaps associated with this workforce.

In addition, the Secret Service did not reliably determine the number of IT staff that it needs in order to support OCIO's functions. Specifically, in January 2017, an independent review of the staffing model that the component used to identify its IT workforce staffing needs found that the model was not based on any verifiable underlying data. In late August 2018, Office of Human Resources officials reported that they had hired a contractor in early August 2018 to update the staffing model to improve the quality of the data. These officials expected the contractor to finish updating the model by August 2019. The officials plan to use the updated model to identify the Secret Service's IT workforce staffing needs for fiscal year 2021. Updating the staffing model to incorporate verifiable workload data should increase the likelihood that the Secret Service is able to appropriately identify its staffing needs for its IT workforce.

- **Regularly assess competency and staffing needs, and analyze the IT workforce to identify gaps in those areas—not implemented.** The Secret Service regularly assessed the competency and staffing needs for 1 of the occupational series within its IT workforce (i.e., the 2210 IT Specialist series). However, it did not regularly assess the competency and staffing needs for the remaining 11 occupational series that are associated with the component's IT workforce, nor identify any gaps that it had in those areas.[41]

  OCIO officials stated that they had not assessed these needs or identified competency or staffing gaps because, among other things, the Secret Service was focused on reorganizing the IT workforce under a single, centralized reporting chain within the CIO's office. However, as previously mentioned, the component completed this effort in March 2017, but OCIO did not subsequently assess its competency and staffing needs, nor identify gaps in those areas.

  OCIO officials reported that they plan to assess the competencies of the IT workforce to identify any gaps that may exist; however, they

[41]Occupational series (also referred to as occupations) are subsets of an occupational group consisting of positions in a similarly specialized line of work and with similar qualification requirements.

were unable to identify a specific date by which they expect to have the capacity to complete this assessment. Until OCIO regularly analyzes the IT workforce to identify its competency needs and any gaps it may have, OCIO will be limited in its ability to determine whether its IT workforce has the necessary knowledge and skills to meet its mission and goals.

Further, Office of Human Resources officials reported that they plan to update the staffing model that they use to identify their IT staffing needs to include more reliable workload data. However, as discussed earlier, the Secret Service had not yet developed that updated model to determine its IT staffing needs. Office of Human Resources officials reported that once they update the staffing model they plan to re-evaluate the Secret Service's IT staffing needs. The officials also stated that, going forward, they plan to reassess these needs each year as part of the annual budget cycle. Regular assessments of the IT workforce's staffing needs should increase the likelihood that the Secret Service is able to appropriately identify the number of IT staff it needs to meet its mission and programmatic goals.

- **Develop strategies and plans to address gaps in competencies and staffing—partly implemented.** The Secret Service developed recruiting and hiring strategies to address certain competency and staffing needs (e.g., cybersecurity) for its IT workforce. These strategies included, among other things, participating in DHS-wide recruiting events and using special hiring authorities.

  However, because OCIO did not identify all of its IT competency and staffing needs, and lacked a current analysis of its entire IT workforce, the Secret Service could not provide assurance that the recruiting and hiring strategies it developed were specifically targeted towards addressing current OCIO competency and staffing gaps. For example, without an analysis of the IT workforce's skills, OCIO did not know the extent to which it had gaps in areas such as device management and cloud computing.[42] As a result, the Secret Service's recruiting strategies may not have been targeted to address any gaps in those areas. Until the Secret Service updates its recruiting and hiring

[42]Cloud computing is a means for enabling on-demand access to shared and scalable pools of computing resources. It enables an agency to purchase IT services through a service provider, rather than paying for all of the assets (e.g., hardware, software, and networks) that would typically be needed to provide such services.

strategies and plans to address all IT competency and staffing gaps identified (after OCIO completes its analysis of the entire IT workforce, as discussed earlier), the Secret Service will be limited in its ability to effectively recruit and hire staff to fill those gaps.

The Secret Service Minimally Implemented Selected Leading Recruitment and Hiring Practices

According to the Office of Personnel Management, the Chief Human Capital Officers Council, and our prior work, once an agency has determined the critical skills and competencies that it needs to achieve programmatic goals, and identifies any competency or staffing gaps in its current workforce, the agency should be positioned to build effective recruiting and hiring programs. It is important that an agency has these programs in place to ensure that it can effectively recruit and hire employees with the appropriate skills to meet its various mission requirements.

The Office of Personnel Management, the Chief Human Capital Officers Council, and we have also identified numerous leading practices associated with effective recruitment and hiring programs.[43] Among these practices, an agency should (1) implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process; (2) establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps; and (3) adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics.

The Secret Service minimally implemented the selected three leading practices associated with the recruitment and hiring workforce area. Specifically, the component partly implemented one of the three practices and did not implement the other two practices. Table 9 lists these selected practices and provides our assessment of the Secret Service's implementation of the practices.

[43]Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative* (September 2008); and GAO-17-8.

Table 9: The U.S. Secret Service's Implementation of Selected Leading Recruitment and Hiring Practices, as of June 2018

Overall workforce area rating	Practice rating		Leading practice
Minimally implemented	Partly implemented	1.	Implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process.
	Not implemented	2.	Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps.
	Not implemented	3.	Adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

- **Implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process—partly implemented.** OCIO officials implemented the activities identified in the Secret Service's recruiting and hiring plans. For example, as identified in its recruiting plan, OCIO participated in a February 2017 career fair to recruit job applicants at a technology conference. In addition, in August 2017, OCIO participated in a DHS-wide recruiting event. Secret Service officials reported that, during this event, they conducted four interviews for positions in OCIO.

  However, as previously discussed, OCIO did not identify all of its IT competency and staffing needs, and lacked a current analysis of its entire IT workforce. Without complete knowledge of its current IT competency and staffing gaps, the Secret Service could not provide assurance that the recruiting and hiring strategies that it had implemented fully addressed these gaps.

- **Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps—not implemented.** The Secret Service had not established and tracked metrics for monitoring the effectiveness of its recruitment and hiring activities for the IT workforce. Officials in the Office of Human Resources attributed this to staffing constraints and said their priority was to address existing staffing gaps associated with the Secret Service's law enforcement groups.

  In June 2018, Office of Human Resources officials stated that they plan to implement metrics to monitor the effectiveness of the hiring

process for the IT workforce by October 2018. The officials also stated that they were in the process of determining (1) the metrics that are to be used to monitor the effectiveness of their workforce recruiting efforts and (2) whether they need to acquire new technology to support this effort. However, the officials did not know when they would implement the metrics for assessing the effectiveness of the recruitment activities and whether they would report the results to leadership.

Until the Office of Human Resources (1) develops and tracks metrics to monitor the effectiveness of the Secret Service's recruitment activities for the IT workforce, including their effectiveness at addressing skill and staffing gaps; and (2) reports to component leadership on those metrics, the Secret Service and the Office of Human Resources will be limited in their ability to analyze the recruitment program to determine whether the program is effectively addressing IT skill and staffing gaps. Further, Secret Service leadership will lack the information necessary to make effective recruitment decisions.

- **Adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics—not implemented.** While the Secret Service CIO stated in June 2018 that he planned to adjust the office's recruiting and hiring strategies to focus on entry-level staff rather than mid-career employees, this planned adjustment was not based on metrics that the Secret Service was tracking. Instead, the CIO stated that he planned to make this change because his office determined that previous mid-career applicants were often unwilling or unable to wait for the Secret Service's lengthy, required background investigation process to be completed.

  However, as previously mentioned, the Secret Service did not develop and implement any metrics for assessing the effectiveness of the recruitment and hiring activities for the IT workforce. As a result, the Office of Human Resources and OCIO were not able to use such metrics to inform adjustments to their recruiting and hiring plan and activities, thus, reducing their ability to target potential candidates for hiring.

  Until the Office of Human Resources and OCIO adjust their recruitment and hiring plans and activities as necessary, after establishing and tracking metrics for assessing the effectiveness of these activities for the IT workforce, the Secret Service will be limited

in its ability to ensure that its recruiting plans and activities are appropriately targeted to potential candidates. In addition, the component will lack assurance that these plans and activities will effectively address skill and staffing gaps within its IT workforce.

The Secret Service Minimally Implemented Selected Leading Training and Development Practices

An organization should invest in training and developing its employees to help ensure that its workforce has the information, skills, and competencies that it needs to work effectively. In addition, training and development programs are an integral part of a learning environment that can enhance an organization's ability to attract and retain employees with the skills and competencies needed to achieve cost-effective and timely results.

DHS, the Secret Service, and we have previously identified numerous leading training and development-related practices. Among those practices, an organization should (1) establish a training and development program to assist the agency in achieving its mission and goals; (2) use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable; and (3) collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.[44]

The Secret Service minimally implemented the selected three leading practices associated with the training and development workforce area. Specifically, the component partly implemented two of the three practices and did not implement one practice. Table 10 lists these selected leading practices and provides our assessment of the Secret Service's implementation of the practices.

[44]DHS, Instruction 102-01-001, *Acquisition Management Instruction* (Mar. 9, 2016); the U.S. Secret Service, *Acquisition Workforce Certification*, ADM-10 (04) (Dec. 19, 2012); and GAO-04-546G.

Table 10: The U.S. Secret Service's Implementation of Selected Leading Training and Development Practices, as of June 2018

Overall workforce area rating	Practice rating	Leading practice
Minimally implemented	Partly implemented	1. Establish a training and development program to assist the agency in achieving its mission and goals.
	Partly implemented	2. Use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable.
	Not implemented	3. Collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

- **Establish a training and development program to assist the agency in achieving its mission and goals—partly implemented.**[45] OCIO was in the process of developing a training program for its IT workforce. For example, OCIO developed a draft training plan that identified recommended training for the office's various IT workforce groups (e.g., voice communications employees).

  However, the office had not defined the required training for each IT workforce group. In addition, OCIO officials had not yet determined which activities they would implement as part of the training program (e.g., soliciting employee feedback after training is completed and evaluating the effectiveness of specific training courses), nor did they implement those activities.

  OCIO officials stated that they had not yet fully implemented a training program because their annual training budget for fiscal year 2018 was not sufficient to implement such a program. However, resource constrained programs especially benefit from identifying and prioritizing training activities to inform training budget decisions. Until OCIO (1) defines the required training for each IT workforce group, (2) determines the activities that it will include in its IT workforce training and development program based on its available training budget, and (3) implements those activities, the office may be limited in its ability to ensure that the IT workforce has the necessary knowledge and skills for their respective positions.

[45]We use "program" to refer to a system of procedures or activities with the purpose of enhancing employees' skills and competencies.

- **Use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable—partly implemented.** OCIO used a training system to track that the managers for IITT's programs had met certain certification requirements for their respective positions. In addition, OCIO manually tracked the technical training that certain IT staff took.

  However, as discussed earlier, OCIO did not define the required training for each IT workforce group. As such, the office was unable to ensure that IT staff received the appropriate training relevant to their respective positions. Until it ensures that IT staff complete training specific to their positions (after defining the training required for each workforce group), OCIO will have limited assurance that the workforce has the necessary knowledge and skills.

- **Collect and assess performance data (including qualitative or quantitative measures, as appropriate[46]) to determine how the training program contributes to improved performance and results—not implemented.** As previously discussed, OCIO did not fully implement a training program for the IT workforce; as such, the office was unable to collect and assess performance data related to such a program. OCIO officials stated that, once they fully implement a training program, they intend to collect and assess data on how this program contributes to improved performance. However, the officials were unable to specify a time frame for when they would do so.

  Until OCIO collects and assesses performance data (including qualitative or quantitative measures, as appropriate) to determine how the IT training program contributes to improved performance and

[46]GAO's *Human Capital Guide for Assessing Strategic Training and Development Efforts* (GAO-04-546G) identifies the following commonly accepted training program evaluation model that consists of five levels of assessment: (1) The first level measures the training participants' reaction to, and satisfaction with, the training program. (2) The second level measures the extent to which learning has occurred because of the training effort. (3) The third level measures the application of the learning to the work environment. (4) The fourth level measures the impact of the training program on the agency's program or organizational results. (5) The fifth level—often referred to as return on investment—compares the benefits (quantified in dollars) to the costs of the training and development program. GAO's guide notes that, when evaluating specific training and development programs, agencies should select the analytical approach that best measures the effect of a training program while also considering what is realistic and reasonable given the broader context of the issue and fiscal constraints.

results (once the training program is implemented), the office may be limited in its knowledge of whether the training program is contributing to improved performance and results.

The Secret Service Substantially Implemented Selected Leading Practices for Improving the Morale of Its IT Workforce, but Did Not Demonstrate Sustained Improvement

Employee morale is important to organizational performance and an organization's ability to retain talent to perform its mission. We have previously identified numerous leading practices for improving employee morale.[47] Among other things, we have found that an organization should (1) determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans; and develop and implement action plans to improve employee morale; (2) establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale; and (3) maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale.[48]

With regard to its IT workforce, the Secret Service substantially implemented the selected three practices associated with the employee morale workforce area. Specifically, the component fully implemented two of the selected practices and partly implemented one practice. Table 11 lists these selected practices and provides our assessment of the Secret Service's implementation of the practices.

[47]GAO-12-940.

[48]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

Table 11: The U.S. Secret Service's Implementation of Selected Leading Practices for Improving the Morale of Its Information Technology (IT) Workforce, as of June 2018

Overall workforce area rating	Practice rating	Leading practice
Substantially implemented[a]	Fully implemented	1. Determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans. Develop and implement action plans to improve employee morale.
	Fully implemented	2. Establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale.
	Partly implemented	3. Maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

[a]While the Secret Service substantially implemented the selected employee morale practices for its IT workforce and the majority of the component's IT staff reported that their morale was "very good" or "excellent" as of December 2017, additional work remains for the Secret Service and the Department of Homeland Security to improve employee morale across the Secret Service and the department.

- **Determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans. Develop and implement action plans to improve employee morale—fully implemented.** The Secret Service used survey analysis techniques to determine the root causes of its low employee morale, on which we have previously reported.[49] For example, the component conducted a benchmarking exercise where it compared the morale of the Secret Service's employees, including IT staff, to data on the morale of employees at other agencies, including the U.S. Capitol Police, U.S. Coast Guard, and the Drug Enforcement Administration. As part of this exercise, the Secret Service also compared its employee work-life offerings (e.g., on-site childcare and telework program) to those available at other agencies.

  In addition, the Secret Service developed and implemented action plans for improving employee morale. Among these action plans, for example, the component implemented a student loan repayment program and expanded its tuition assistance program's eligibility requirements.

[49]GAO-12-940.

- **Establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale—fully implemented.** The Secret Service tracked metrics for improving employee morale and reported the results to leadership. For example, the component tracked metrics on the percentage of the workforce, including IT staff, that participated in the student loan repayment and tuition assistance programs. In addition, the Chief Strategy Officer reported to the Chief Operating Officer the results related to meeting those metrics.

- **Maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale—partly implemented.** Secret Service leadership developed and implemented initiatives that demonstrated their commitment to improving the morale of the Secret Service's workforce. For example, since 2014, the Secret Service had worked with a contractor to identify ways to improve the morale of its entire workforce, including IT staff.

  However, as of June 2018, the Secret Service was unable to demonstrate that it had sustained improvement in the morale of the component's IT staff. In particular, the component was only able to provide IT workforce-specific results from one employee morale assessment that was conducted subsequent to the consolidation of this workforce into OCIO in March 2017. These results were from an assessment conducted by the component's Inspection Division in December 2017 (the assessment found that the majority of the Secret Service's IT employees rated their morale as "very good" or "excellent.")

  While the component also provided certain employee morale results from the Office of Personnel Management's Federal Employee Viewpoint Survey[50] in 2017, these results were not specific to the IT workforce. Instead, this workforce's results were combined with those from staff in another Secret Service division. According to OCIO officials, the results were combined because, at the time of the survey, the IT workforce was administratively identified as being part of that other division.

[50]The Office of Personnel Management's Federal Employee Viewpoint Survey is a tool that measures employees' perceptions of whether and to what extent conditions characterizing successful organizations are present in their agency.

OCIO officials stated that, going forward, they plan to continue to assess the morale of the IT workforce on an annual basis as part of the Federal Employee Viewpoint Survey. In addition, the officials stated that OCIO-specific results may be available as part of the 2018 survey results, which the officials expect to receive by September 2018. By measuring employee satisfaction on an annual basis, the Secret Service should have increased knowledge of whether its initiatives that are aimed at improving employee morale are in fact increasing employee satisfaction.

The Secret Service Substantially Implemented Selected Performance Management Leading Practices, but Did Not Explicitly Align Expectations with Organizational Goals

Agencies can use performance management systems as a tool to foster a results-oriented organizational culture that links individual performance to organizational goals. We have previously identified numerous leading practices related to performance management that are intended to enhance performance and ensure individual accountability.[51] Among the performance management practices, agencies should (1) establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance, (2) explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals, and (3) periodically provide individuals with regular performance feedback.

The Secret Service substantially implemented the selected three leading practices associated with the performance management workforce area. Specifically, the component fully implemented one of the three practices and partly implemented the other two practices. Table 12 lists these selected leading practices and provides our assessment of the Secret Service's implementation of the practices.

[51]GAO-03-488.

Table 12: The U.S. Secret Service's Implementation of Selected Leading Performance Management Practices, as of June 2018

Overall workforce area rating	Practice rating	Leading practice
Substantially implemented	Partly implemented	1. Establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance.
	Partly implemented	2. Explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals.
	Fully implemented	3. Periodically provide individuals with regular performance feedback.

Source: GAO analysis of data provided by U.S. Secret Service officials. | GAO-19-60.

- **Establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance—partly implemented.** The Secret Service's performance management process requires leadership to make meaningful distinctions between levels of staff performance. In particular, the component's performance plans for IT staff, which are developed by the Office of Human Resources and tailored by OCIO, as necessary, specify the criteria that leadership use to determine if an individual has met or exceeded the expectations associated with each competency identified in their respective performance plan. The performance plans include pre-established, department-wide competencies that are set by DHS, as well as occupational series-specific goals that may be updated by the Secret Service.

  However, because OCIO did not fully define and document all of its technical competency needs for the IT workforce, as discussed earlier, the Secret Service's performance plans for IT staff did not include performance expectations related to the full set of technical competencies required for their respective positions. In addition, because OCIO officials were unable to specify a time frame for when they will identify all of the technical competency needs for the IT workforce (as previously discussed), the officials were also unable to specify a time frame for when they would update the IT workforce's performance plans to include those relevant technical competencies.

  Until OCIO updates the performance plans for each occupational series within the IT workforce to include the relevant technical competencies, once identified, against which IT staff performance should be assessed, the office will be limited in its ability to provide IT staff with a complete assessment of their performance. In addition,

Secret Service management will have limited knowledge of the extent to which IT staff are meeting all relevant technical competencies.

- **Explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals—partly implemented.** The Secret Service's performance plans for IT staff identified certain goals that appeared to be related to organizational goals and objectives. For example, the performance plan for the Telecommunications Specialist occupational series (which is one of the series included in OCIO's IT workforce) identified a goal for staff to support the voice, wireless, radio, satellite, and video systems serving the Secret Service's protective and investigative mission. This performance plan goal appeared to be related to the component's strategic goal on Advanced Technology, which included an objective to create the infrastructure needed to fulfill mission responsibilities.

  However, the Secret Service was unable to provide documentation that explicitly showed how individual employee performance links to organizational goals, such as a mapping of the goals identified in employee performance plans to organizational goals. Specifically, while Office of Human Resources officials stated that each Secret Service directorate is responsible for ensuring that employee goals map to high-level organizational goals, OCIO officials stated that they did not complete this mapping. The officials were unable to explain why they did not align the goals in their employees' performance plans to the component's high-level goals.

  According to the officials, the Secret Service is in the process of implementing a new automated tool that will require each office to explicitly align individual performance expectations to organizational goals. The officials stated that OCIO plans to use this tool to create employees' fiscal year 2019 performance plans. By explicitly demonstrating how individual performance expectations align with organizational goals, the Secret Service's IT staff should have a better understanding of how their daily activities contribute towards achieving the Secret Service's goals.

- **Periodically provide individuals with regular performance feedback—fully implemented.** Secret Service leadership periodically provided their IT staff with performance feedback. Specifically, on an annual basis, OCIO staff received feedback during a mid-year and end-of-year performance feedback assessment. In our prior work, we

have stressed that candid and constructive feedback can help individuals maximize their contribution and potential for understanding and realizing the goals and objectives of an organization. Further, this feedback is one of the strongest drivers of employee engagement.[52]

The Secret Service and DHS Implemented Selected Leading Monitoring Practices for the IITT Investment

According to leading practices of the Software Engineering Institute, effective program oversight includes monitoring program performance and conducting reviews at predetermined checkpoints or milestones. This is done by, among other things, comparing actual cost, schedule, and performance data with estimates in the program plan and identifying significant deviations from established targets or thresholds for acceptable performance levels.[53]

In addition, the Software Engineering Institute previously identified leading practices for effectively monitoring the performance of agile projects.[54] According to the Institute, agile development methods focus on delivering usable, working software frequently; as such, it is important to measure the value delivered during each iteration of these projects. To that end, the Institute reported that agile projects should be measured on velocity (i.e., number of story points[55] completed per sprint[56] or release),

[52]See, for example, GAO, *Federal Workforce: Additional Analysis and Sharing of Promising Practices Could Improve Employee Engagement and Performance,* GAO-15-585 (Washington, D.C.: July 14, 2015); and GAO-03-488.

[53]Software Engineering Institute, *CMMI® for Acquisition, Version 1.3, Project Monitoring and Control* process area (Pittsburgh, PA: November 2010).

[54]Software Engineering Institute, *Agile Metrics: Progress Monitoring of Agile Contractors*, CMU/SEI-2013-TN-029 (January 2014).

[55]In agile development, user stories convey the customers' requirements at the smallest and most discrete unit of work that must be done to create working software. Each user story is assigned a level of effort, called story points, which is a relative unit of measure used to communicate complexity and progress between the business and development sides of the project.

[56]A sprint is a set period of time, for example, two weeks, during which the development team is expected to complete tasks (i.e., user stories) related to the development of an increment of software.

development progression (e.g., the number of user stories[57] planned and accepted), product quality (e.g., number of defects), and post-deployment user satisfaction.

DHS and the Secret Service had fully implemented the selected leading practice[58] for monitoring the performance of one program and three projects[59] within the IITT investment,[60] and conducting reviews of this program and these projects at predetermined checkpoints.[61] In addition, with regard to the selected leading practice for monitoring agile projects,[62] the Secret Service had fully implemented this practice for one of its two projects being implemented using agile and had partially implemented this practice for the other project. Table 13 provides a summary of DHS's and the Secret Service's implementation of these leading practices, as relevant for one program and three projects within IITT.

[57]User stories convey the customers' requirements at the smallest and most discrete unit of work that must be done to create working software.

[58]This selected practice is a combination of four practices identified by the Software Engineering Institute that were associated with monitoring program performance and progress. We combined these four practices into one practice.

[59]Two of these projects—Uniformed Division Resource Management System and Events Management—were projects within IITT's Enterprise Resource Management System program. The third project—Multi-Level Security—was a standalone project that was not part of another IITT program.

[60]As of June 2018, IITT's Enterprise-wide Scheduling project—which was part of the Enterprise Resource Management System program—was still in the planning phase; as such, we did not review it.

[61]As previously discussed, both DHS and the Secret Service are responsible for providing oversight to the Enabling Capabilities program, which is a major acquisition program within IITT. DHS's Under Secretary for Management delegated oversight of IITT's non-major projects—including Multi-Level Security, Uniformed Division Resource Management System, and Events Management—to the Secret Service Component Acquisition Executive.

[62]This selected practice is a combination of four agile metrics that the Software Engineering Institute identified as important for successful agile implementations. We combined these four practices into one practice.

Table 13: Department of Homeland Security's and the U.S. Secret Service's Implementation of Selected Leading Practices for Monitoring the Performance of One Program and Three Projects within the Information Integration and Technology Transformation Investment

Leading practice	Enabling Capabilities program	Multi-Level Security project	Uniformed Division Resource Management System project[a]	Events Management project[a]
1. Monitor program performance and conduct reviews at predetermined checkpoints or milestones by, among other things, comparing actual cost, schedule, and performance data with estimates in the program plan and identifying significant deviations from established targets or thresholds for acceptable performance levels.	Fully implemented	Fully implemented	Fully implemented	Fully implemented
2. Measure and monitor agile projects on velocity (i.e., number of story points completed per sprint or release), development progression (e.g., the number of features and user stories planned and accepted), product quality (e.g., number of defects), and post-deployment user satisfaction.	Not applicable[b]	Not applicable[b]	Partly implemented [c]	Fully implemented

Source: GAO analysis of data provided by officials from the U.S. Secret Service and Department of Homeland Security. | GAO-19-60.

[a]The Uniformed Division Resource Management System and Events Management projects were part of the Enterprise Resource Management System program within the Information Integration and Technology Transformation investment.

[b]The Secret Service was not implementing the Enabling Capabilities program or Multi-Level Security project using an agile methodology.

[c]The agile metrics that were applicable to the Uniformed Division Resource Management System—which had been deployed to users—were velocity, development progression, product quality, and post-deployment user satisfaction.

[d]The agile metrics that were applicable to Events Management—which had not yet been deployed to users, as of early May 2018—were velocity and development progression.

- **Monitor program performance and conduct reviews at predetermined checkpoints or milestones.** Consistent with leading practices, DHS and the Secret Service monitored the performance of IITT's program and projects by comparing actual cost, schedule, and performance information against planned targets and conducting reviews at predetermined checkpoints. For example, within the Secret Service:

  - The Enabling Capabilities program and Multi-Level Security project monitored their contractors' costs spent to-date on a monthly basis and compared them to the total contract amounts.

  - OCIO used integrated master schedules to monitor the schedule performance of the Enabling Capabilities program and Multi-Level Security project.

- OCIO also monitored the cost, schedule, and performance of the Uniformed Division Resource Management System and Events Management projects during monthly status reviews.

In addition, DHS and the Secret Service conducted acquisition decision event reviews and systems engineering life cycle technical reviews of IITT's program and projects at predetermined checkpoints and, when applicable, identified deviations from established cost, schedule, and performance targets. For example:

- Secret Service OCIO met with DHS's Office of Program Accountability and Risk Management in February 2017, and with DHS's Acting Under Secretary for Management in June 2017, to discuss a schedule breach for the Enabling Capabilities program. In particular, the Enabling Capabilities program informed DHS that the program needed to change the planned date for acquisition decision event 3 (the point at which a decision is made to fully deploy the system) in order to conduct tests in an operational environment prior to that decision event. This delay was due to the Secret Service misunderstanding the tests that it was required to conduct prior to that decision event. Specifically, the Enabling Capabilities program had conducted tests on "production representative" systems, but these tests were not sufficient to meet the requirements for acquisition decision event 3.

- The project team for Multi-Level Security identified that certain technical issues they had experienced would delay system deployment and full operational capability (the point at which an investment becomes fully operational). As such, in October 2017, the project notified the Secret Service Component Acquisition Executive of these expected delays.[63] In particular, the web browser that was intended to provide users on "Sensitive But Unclassified" workstations the ability to view information from different security levels, experienced technical delays in meeting personal identity verification requirements. The project team also described for the executive how the schedule delay would affect the project's performance metrics and funding, and subsequently updated the project plan accordingly.

[63]As previously discussed, the Component Acquisition Executive is the senior acquisition official within a component that is responsible for implementation, management, and oversight of the component's acquisition process.

- **Measure and monitor agile projects on, among other things, velocity (i.e., number of story points completed per sprint or release), development progression (e.g., the number of features and user stories planned and accepted), product quality (e.g., number of defects), and post-deployment user satisfaction.** Secret Service OCIO measured its two agile projects—Uniformed Division Resource Management System and Events Management—using certain agile metrics. In particular, OCIO officials measured the Uniformed Division Resource Management System and Events Management projects using key metrics related to velocity and development progression. For example, the officials measured development progression for both projects on a daily basis. In addition, OCIO officials monitored each project's progress against these metrics during bi-weekly reviews that they conducted with each project team.

  The OCIO officials also tracked product quality metrics for the Uniformed Division Resource Management System.[64] For example, on a monthly basis, the officials tracked the number of helpdesk tickets that had been resolved related to the system. In addition, on a quarterly basis, they tracked the number of Uniformed Division Resource Management System defects that (1) had been fixed and (2) were in the backlog.

  However, while OCIO officials received certain post-deployment user satisfaction information from end-users of the Uniformed Division Resource Management System by, among other things, tracking the number of helpdesk tickets related to the system and via daily verbal, undocumented feedback from certain Uniformed Division officers, OCIO officials had not fully measured and documented post-deployment user satisfaction with the system, such as via a survey of employees who use the system. The officials stated that they had not conducted and documented a survey because they were focused on (1) addressing software performance issues that occurred after they deployed the system to a limited number of users, and (2) continuing system deployment to the remaining users after they addressed the performance issues.

[64]Product quality (e.g., number of defects) and post-deployment user satisfaction are measured after a system has been deployed to users. The Events Management system had not yet been deployed to users, as of early May 2018; as such, these metrics were not yet applicable to the project.

OCIO officials stated that they plan to conduct such a documented survey by the end of September 2018. The results of the user satisfaction survey should provide OCIO with important information on whether the Uniformed Division Resource Management System is meeting users' needs.

Conclusions

The Secret Service's full implementation of 11 of 14 component-level CIO responsibilities constitutes a significant effort to establish CIO oversight for the component's IT portfolio. Additional efforts to fully implement the remaining 3 responsibilities, including ensuring that all IT contracts are reviewed, as appropriate; ensuring that the Secret Service's enterprise governance policy appropriately specifies the CIO's role in developing and reviewing the component's IT budget formulation and execution; and ensuring agile projects measure product quality and post-deployment user satisfaction, will further position the CIO to effectively manage the Secret Service's IT portfolio.

When effectively implemented, IT workforce planning and management activities can facilitate the successful accomplishment of an agency's mission. However, the Secret Service had not fully implemented all of the 15 selected practices for its IT workforce for any of the five areas—strategic planning, recruitment and hiring, training and development, employee morale, and performance management. The Secret Service's lack of (1) a strategic workforce planning process, including the identification of all required knowledge and skills, assessment of competency gaps, and targeted strategies to address specific gaps in competencies and staffing; (2) targeted recruiting activities, including metrics to monitor the effectiveness of the recruitment program and adjustment of the recruitment program and hiring efforts based on metrics; (3) a training program, including the identification of required training for IT staff, ensuring that staff take required training, and assessment of performance data regarding the training program; and (4) a performance management system that includes all relevant technical competencies, greatly limits its ability to ensure the timely and effective acquisition and maintenance of the Secret Service's IT infrastructure and services.

On the other hand, by monitoring program performance and conducting reviews at predetermined checkpoints for one program and three projects associated with the IITT investment, in accordance with leading practices,

the Secret Service and DHS provided important oversight needed to guide that program and those projects. Measuring projects on leading agile metrics also provided the Secret Service CIO with important information on project performance.

Recommendations for Executive Action

We are making the following 13 recommendations to the Director of the Secret Service:

The Director should ensure that the CIO establishes and documents an IT acquisition review process that ensures the CIO or the CIO's delegate reviews all contracts containing IT, as appropriate. (Recommendation 1)

The Director should update the enterprise governance policy to specify (1) the CIO's current role and responsibilities on the Executive Resources Board, to include developing and reviewing the IT budget formulation and execution; and (2) the Deputy CIO's role and responsibilities on the Enterprise Governance Council. (Recommendation 2)

The Director should ensure that the Secret Service develops a charter for its Executive Resources Board that specifies the roles and responsibilities of all board members, including the CIO. (Recommendation 3)

The Director should ensure that the CIO includes product quality and post-deployment user satisfaction metrics in the modular outcomes and target measures that the CIO sets for monitoring agile projects. (Recommendation 4)

The Director should ensure that the CIO identifies all of the required knowledge and skills for the IT workforce. (Recommendation 5)

The Director should ensure that the CIO regularly analyzes the IT workforce to identify its competency needs and any gaps it may have. (Recommendation 6)

The Director should ensure that, after OCIO completes an analysis of the IT workforce to identify any competency and staffing gaps it may have, the Secret Service updates its recruiting and hiring strategies and plans to address those gaps, as necessary. (Recommendation 7)

The Director should ensure that the Office of Human Resources (1) develops and tracks metrics to monitor the effectiveness of the Secret Service's recruitment activities for the IT workforce, including their effectiveness at addressing skill and staffing gaps; and (2) reports to component leadership on those metrics. (Recommendation 8)

The Director should ensure that the Office of Human Resources and OCIO adjust their recruitment and hiring plans and activities, as necessary, after establishing and tracking metrics for assessing the effectiveness of these activities for the IT workforce. (Recommendation 9)

The Director should ensure that the CIO (1) defines the required training for each IT workforce group, (2) determines the activities that OCIO will include in its IT workforce training and development program based on its available training budget, and (3) implements those activities. (Recommendation 10)

The Director should ensure that the CIO ensures that the IT workforce completes training specific to their positions (after defining the training required for each workforce group). (Recommendation 11)

The Director should ensure that the CIO collects and assesses performance data (including qualitative or quantitative measures, as appropriate) to determine how the IT training program contributes to improved performance and results (once the training program is implemented). (Recommendation 12)

The Director should ensure that the CIO updates the performance plans for each occupational series within the IT workforce to include the relevant technical competencies, once identified, against which IT staff performance should be assessed. (Recommendation 13)

Agency Comments and Our Evaluation

DHS provided written comments on a draft of this report, which are reprinted in appendix III. In its comments, the department concurred with all 13 of our recommendations and provided estimated completion dates for implementing each of them.

For example, with regard to recommendation 2, the department stated that the Secret Service would update its enterprise governance policy and related policies to outline the roles and responsibilities of the CIO and

Deputy CIO, among others, by March 31, 2019. In addition, for recommendation 13, the department stated that the Secret Service OCIO will include relevant technical competencies in performance plans, as appropriate, in the next performance cycle that starts in July 2019. If implemented effectively, these actions should address the weaknesses we identified.

The department also identified a number of other actions that it said had been taken to address our recommendations. For example, in response to recommendation 8, which calls for the Office of Human Resources to (1) develop and track metrics to monitor the effectiveness of the Secret Service's recruitment activities for the IT workforce and (2) report to component leadership on those metrics, DHS stated that the Secret Service's Office of Human Resources' Outreach Branch provides to the department metrics on recruitment efforts toward designated priority mission-critical occupations.

However, for fiscal year 2017, only 1 of the 12 occupational series associated with the Secret Service's IT workforce was designated as a mission-critical occupation for the component (i.e., the 2210 IT Specialist series). The 11 other occupational series were not designated as mission-critical occupations. In addition, for fiscal year 2018, none of these 12 occupational series were designated as mission-critical occupations. As such, metrics on recruiting for these IT series may not have been reported to DHS leadership.

Moreover, while we requested documentation of the recruiting metrics for the Secret Service's IT workforce and, during the course of our review, had multiple subsequent discussions with the Secret Service regarding such metrics, the component did not provide documentation that demonstrated it had established recruiting metrics for its IT workforce. Tracking such metrics and reporting the results to Secret Service leadership, as we recommended, would provide management with important information necessary to make effective recruitment decisions.

Further, in response to recommendation 10, which among other things, calls for the CIO to define the required training for each IT workforce group, the department stated that the Secret Service OCIO recently developed training requirements for each workforce group, which were issued during our audit. However, while during our audit OCIO provided a list of recommended training courses, the office did not identify them as being required courses. Defining training that is required for each IT workforce group, as we recommended, would inform OCIO of the

necessary training for each position and enable the office to prioritize this training, to ensure that its staff have the needed knowledge and skills.

In addition to the aforementioned comments, we received technical comments from DHS and Secret Service officials, which we incorporated, as appropriate.

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

Should you or your staffs have any questions on information discussed in this report, please contact me at (202) 512-4456 or HarrisCC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Carol C. Harris
Director, Information Technology Acquisition Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to evaluate the extent to which: (1) the U.S. Secret Service (Secret Service) Chief Information Officer (CIO)[1] has implemented selected information technology (IT) oversight responsibilities, (2) the Secret Service has implemented leading workforce planning and management practices for its IT workforce, and (3) the Secret Service and the Department of Homeland Security (DHS) have implemented selected performance and progress monitoring practices for the Information Integration and Technology Transformation (IITT) investment.

To address the first objective, we analyzed DHS's policies and guidance on IT management to identify the responsibilities that were to be implemented by the component-level CIO related to overseeing the Secret Service's IT portfolio, including existing systems, acquisitions, and investments.[2] From the list of 33 responsibilities that we identified, we then excluded the responsibility that was associated with information security, which is expected to be addressed as part of a separate, subsequent GAO review. We also excluded those responsibilities that were significantly large in scope (e.g., implement an enterprise architecture) or that, in our professional judgment, lacked specificity (e.g., provide timely delivery of mission IT services). As a result, we excluded from consideration for this review a total of 10 CIO responsibilities.

For the 23 that remained, we then combined certain responsibilities that overlapped with other related responsibilities. For example, we combined related responsibilities on the component CIO's review of IT contracts. As

[1]Throughout this appendix, CIO and OCIO respectively refer to the Secret Service Chief Information Officer and Secret Service Office of the Chief Information Officer unless otherwise specified.

[2]These policies and guidance included: DHS, Instruction 102-01-004, *Agile Development and Delivery for Information Technology* (April 2016); Instruction 102-02-001, *Capital Planning and Investment Control Guidebook* (March 2016); Directive 102-02, *Capital Planning and Investment Control* (February 2016); Instruction 102-01-103, *Systems Engineering Life Cycle* (November 2015); Directive 142-02, *Information Technology Integration and Management* (February 2014 and updated in April 2018).

a result, we identified 14 responsibilities for review. We validated with the acting DHS CIO that these responsibilities were key responsibilities for the department's component-level CIOs. We then included all 14 of the responsibilities in our review.

The 14 selected component-level CIO responsibilities were:

1. Develop and review the component IT budget formulation and execution.
2. Manage the component IT investment portfolio, including establishing an IT acquisition review process that enables component and DHS review of component acquisitions (i.e., contracts) that contain IT.
3. Develop, implement, and maintain a detailed IT strategic plan.
4. Ensure all component IT policies are in compliance and alignment with DHS IT directives and instructions.
5. Concur with each program's and/or project's systems engineering life cycle tailoring plan.
6. Support the Component Acquisition Executive to ensure processes are established that enable systems engineering life cycle technical reviews and that they are adhered to by programs and/or projects.
7. Ensure that all systems engineering life cycle technical review exit criteria are satisfied for each of the component's IT programs and/or projects.
8. Ensure the necessary systems engineering life cycle activities have been satisfactorily completed as planned for each of the component's IT programs and/or projects.
9. Concur with the systems engineering life cycle technical review completion letter for each of the component's IT programs and/or projects.
10. Maintain oversight of their component's agile development approach for IT by appointing the responsible personnel, identifying investments for adoption, and reviewing artifacts.
11. With Component Acquisition Executives, evaluate and approve the application of agile development for IT programs consistent with the component's agile development approach.
12. Set modular outcomes and target measures to monitor the progress in achieving agile implementation for IT programs and/or projects within their component.

13. Participate on DHS's CIO Council, Enterprise Architecture Board, or other councils/boards as appropriate, and appoint employees to serve when necessary.
14. Meet the IT competency requirements established by the DHS CIO, as required in the component CIO's performance plan.

To determine the extent to which the Secret Service CIO has implemented these responsibilities, we obtained and assessed relevant component documentation and compared it to the responsibilities. Specifically, we obtained and analyzed documentation including evidence of the CIO's participation on the Secret Service governance board that has final decision authority and responsibility for enterprise governance, including the IT budget; monthly program management reports showing the CIO's oversight of IT programs, projects, and systems; monthly status reports on program spending; the Secret Service's IT strategic plan; the Secret Service's enterprise governance policy; meeting minutes from the DHS board and council on which the CIO participated (i.e., the CIO Council and Enterprise Architecture Board); and documentation demonstrating whether the CIO met the IT competency requirements.

In addition, we obtained and analyzed relevant documentation related to the CIO's oversight of the major IT investments on which the Secret Service was spending development, modernization, and enhancement funds during fiscal year 2017. As of July 2017, the component had one investment—IITT—that met this criterion. IITT is a portfolio investment that, as of July 2017, included two programs (one of which included three projects) and one standalone project (i.e., it was not part of another program) that had capabilities that were in planning or development and modernization: the Enabling Capabilities program, Enterprise Resource Management System program (which included three projects, called Uniformed Division Resource Management System, Events Management, and Enterprise-wide Scheduling), and Multi-Level Security project.

In particular, we obtained and analyzed documentation related to the CIO's oversight of the systems engineering life cycles for IITT's Enabling Capabilities program and the Uniformed Division Resource Management System, Events Management, and Multi-Level Security projects.[3] This

[3]The Enterprise-wide Scheduling project within the Enterprise Resource Management System program was still in the planning phase, as of June 2018. As such, we did not review it. We also did not review the Enterprise Resource Management System at the program level.

documentation included acquisition program baselines, systems engineering life cycle tailoring plans, and systems engineering life cycle technical review briefings and completion letters. We then compared the documentation against the five selected systems engineering life cycle oversight responsibilities (responsibilities 5, 6, 7, 8, and 9).

We also obtained and analyzed documentation related to the CIO's oversight of two projects that the Secret Service was implementing using an agile methodology—Uniformed Division Resource Management System and Events Management.[4] Specifically, we obtained and assessed documentation of (1) the CIO's approval for these projects to be implemented using an agile methodology and (2) the agile development metrics that the CIO established for each of these projects. We then compared this documentation to the three agile development-related component-level CIO responsibilities (responsibilities 10, 11, and 12).

Further, to determine the extent to which the Secret Service CIO had established an IT acquisition (i.e., contract) review process that enabled component and DHS review of component contracts that contain IT (which is part of responsibility 2), we first asked Secret Service officials to provide us with a list of all new, unclassified IT contracts that the component awarded between October 1, 2016, and June 30, 2017. The Secret Service officials provided a list of 54 contracts. We validated that these were contracts for IT or IT services by: (1) searching for them in the Federal Procurement Data System – Next Generation;[5] (2) identifying their associated product or service codes, as reported in that system;[6] and (3) determining whether those codes were included in the universe of

[4]The Secret Service also planned to implement the Enterprise-wide Scheduling project using an agile methodology. However, as previously discussed, this project was still in the planning phase, as of June 2018.

[5]The Federal Procurement Data System – Next Generation is a publicly-accessible, web-based tool in which agencies are to report contract transactions.

[6]A product or service code is the category that best identifies the product or service procured.

79 IT product or service codes identified by the Category Management Leadership Council.[7]

In validating the list of 54 contracts provided by the Secret Service, we determined that 5 of the contracts were not associated with an IT product or service code. As such, we removed those contracts from the list. In addition, we found that three other items identified by the component were not in the Federal Procurement Data System – Next Generation. Secret Service officials subsequently confirmed that these three items were not contracts. We therefore removed these three items from the list. As such, the final list of validated contracts identified by the Secret Service included 46 IT contracts.

In addition, to identify any IT contracts that were not included in the list provided by the Secret Service, we conducted a search of the Federal Procurement Data System – Next Generation to identify all unclassified contracts that (1) the component awarded between October 1, 2016, and June 30, 2017; (2) were not a modification of a contract; and (3) were associated with 1 of the 79 IT product or service codes identified by the Category Management Leadership Council. Based on these criteria, we identified 144 Secret Service IT contracts in the Federal Procurement Data System – Next Generation (these 144 contracts included the 46 contracts previously identified by Secret Service officials). We then asked Secret Service officials to validate the accuracy, completeness, and reliability of these data, which they did.

From each of these two lists of IT contracts (i.e., the list of 46 IT contracts identified by the Secret Service and the list of 144 IT contracts that we identified from the Federal Procurement Data System – Next Generation), we then selected random, non-generalizable samples of contracts, as described below.

- First, from the list of 46 IT contracts identified by Secret Service officials, we removed 4 contracts that had total values of less than $10,000. To ensure that we selected across all contract sizes, we

[7]The Category Management Leadership Council is a council of representatives that come from the agencies who comprise the majority of federal procurement spending. The council is chaired by the Administrator of Federal Procurement Policy and it has representatives from the Departments of Defense, Energy, Health and Human Services, Homeland Security, Veterans Affairs, the General Services Administration, the National Aeronautics and Space Administration, and the Small Business Administration.

randomly selected 12 contracts from the remaining list of 42 contracts, using the following cost ranges:

  - $10,000 to $50,000 (4 contracts),
  - more than $50,000 to less than $250,000 (4 contracts), and
  - more than $250,000 (4 contracts).
- Second, from our list of 144 IT contracts that we identified from the Federal Procurement Data System – Next Generation, we removed the 46 contracts identified by Secret Service officials. We also removed 12 contracts that had total values of less than $10,000. To ensure that we selected across all contract sizes, we randomly selected 21 contracts from the remaining list of 86 contracts, using the following cost ranges:
  - $10,000 to $50,000 (7 contracts),
  - more than $50,000 to less than $250,000 (7 contracts), and
  - more than $250,000 (7 contracts).

In total, we selected 33 IT contracts for review. We separated the contracts into the three cost ranges identified above in order to ensure that contracts of different value levels had been selected. This enabled us to determine the extent to which the CIO appropriately reviewed contracts of all values.

To determine the extent to which the CIO had established an IT contract approval process that enabled the Secret Service and DHS, as appropriate, to review IT contracts, we first asked Secret Service Office of the CIO (OCIO) officials for documentation of their IT contract approval process. These officials were unable to provide such documentation. Instead, the officials stated that the Secret Service CIO or the CIO's delegate approves all IT contracts prior to award. The officials also provided documentation that identified four staff to whom the CIO had delegated his approval authority. Further, the officials stated that, in accordance with DHS's October 2016 IT acquisition review guidance, they submitted to DHS OCIO for approval any IT contracts that met DHS's thresholds for review, including those that (1) had total estimated

procurement values of $2.5 million or more, and (2) were associated with a major investment.[8]

Based on the IT acquisition review process that Secret Service OCIO officials described, we then obtained and analyzed each of the 33 selected IT contracts and associated approval documentation to determine whether or not the Secret Service CIO or the CIO's delegate had approved each of the contracts. In particular, we (1) reviewed the name of the contract approver on the approval documentation, and (2) compared the signature dates that were on the contracts to the signature dates that were identified on the associated approval documentation.

In addition, to determine whether or not the Secret Service CIO submitted to DHS OCIO for approval the IT contracts that (1) had total estimated procurement values of $2.5 million or more, and (2) were associated with major investments, we first analyzed the 144 Secret Service IT contracts that we had previously pulled from the Federal Procurement Data System – Next Generation to determine which contracts met the $2.5 million threshold. We identified 4 contracts that met this threshold. We then requested that OCIO identify the levels (i.e., major or non-major) of the investments associated with these contracts. According to OCIO officials, 3 of the 4 contracts were associated with non-major investments and 1 was not associated with an investment.[9] As such, based on DHS's October 2016 IT acquisition review guidance, none of these contracts needed to be submitted to DHS OCIO for review.

We also interviewed Secret Service officials, including the CIO and Deputy CIO, regarding the CIO's implementation of the 14 selected component-level responsibilities. We assessed the evidence against the selected responsibilities to determine the extent to which the CIO had implemented them.

[8]In March 2017, DHS revised its guidance regarding which IT contracts need to be submitted to DHS headquarters for review. This change was made in the middle of the time period from which we selected the contracts in our sample (i.e., October 2016 through June 2017). For the purposes of this review, we evaluated the Secret Service against the department's October 2016 guidance when determining which contracts the Secret Service needed to submit to DHS headquarters for review.

[9]According to Secret Service OCIO officials, the contract that was not associated with an investment was a competitive procurement from wireless service providers.

To address the second objective—determining the extent to which the Secret Service had implemented leading workforce planning and management practices for its IT workforce[10]—we first identified seven topic areas associated with human capital management based on the following sources:

- The Office of Personnel Management's Human Capital Framework.[11]
- Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative*.[12]
- GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others.*[13]
- GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*.[14]
- GAO, *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans*.[15]
- GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*.[16]

[10]As defined by Secret Service OCIO officials, the IT workforce includes government employees who provide direct and indirect support of the day-to-day operations of the Secret Service's enterprise systems and services.

[11]5 C.F.R. pt. 250, subpt. B.

[12]Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative* (September 2008).

[13]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[14]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[15]GAO, *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans,* GAO-12-940 (Washington, D.C.: Sept. 28, 2012).

[16]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government (Supersedes* GAO-03-893G*),* GAO-04-546G (Washington, D.C.: Mar. 1, 2004).

- GAO, *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*.[17]
- DHS acquisition guidance.[18]
- Secret Service acquisition guidance.[19]

Among these topic areas, we then selected five areas that, in our professional judgment, were of particular importance to successful workforce planning and management. They were also previously identified as part of our high-risk and key issues work on human capital management. These areas include: (1) strategic planning, (2) recruitment and hiring, (3) training and development, (4) employee morale, and (5) performance management.

We also reviewed these same sources and identified numerous leading practices associated with the five topic areas. Among these leading practices, we then selected three leading practices within each of the five areas (for a total of 15 selected practices). The selected practices were foundational practices that, in our professional judgment, were of particular importance to successful workforce planning and management.

Table 14 identifies the five selected workforce areas and 15 selected associated practices.

[17]GAO, *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success,* GAO-03-488 (Washington, D.C.: Mar. 14, 2003).

[18]DHS, Instruction 102-01-001, *Acquisition Management Instruction* (Mar. 9, 2016).

[19]The U.S. Secret Service, *Acquisition Workforce Certification,* ADM-10 (04) (Dec. 19, 2012).

Table 14: Selected Workforce Planning and Management Areas and Selected Associated Practices

Workforce area	Selected practice
1. Strategic planning	1. Establish and maintain a strategic workforce planning process, including developing all competency and staffing needs.
	2. Regularly assess competency and staffing needs, and analyze the information technology workforce to identify gaps in those areas.
	3. Develop strategies and plans to address gaps in competencies and staffing.
2. Recruitment and hiring	4. Implement recruiting and hiring activities to address skill and staffing gaps by using the strategies and plans developed during the strategic workforce planning process.
	5. Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps.
	6. Adjust recruitment plans and hiring activities based on recruitment and hiring effectiveness metrics.
3. Training and development	7. Establish a training and development program to assist the agency in achieving its mission and goals.
	8. Use tracking and other control mechanisms to ensure that employees receive appropriate training and meet certification requirements, when applicable.
	9. Collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.
4. Employee morale	10. Determine root causes of employee morale problems by analyzing employee survey results using techniques such as comparing demographic groups, benchmarking against similar organizations, and linking root cause findings to action plans. Develop and implement action plans to improve employee morale.
	11. Establish and track metrics of success for improving employee morale, and report to agency leadership on progress improving morale.
	12. Maintain leadership support and commitment to ensure continued progress in improving employee morale, and demonstrate sustained improvement in morale.
5. Performance management	13. Establish a performance management system that differentiates levels of staff performance and defines competencies in order to provide a fuller assessment of performance.
	14. Explicitly align individual performance expectations with organizational goals to help individuals see the connection between their daily activities and organizational goals.
	15. Periodically provide individuals with regular performance feedback.

Source: GAO analysis of workforce-related areas and practices identified in federal and agency guidance, and GAO's prior work. | GAO-19-60.

To determine the extent to which the Secret Service had implemented the selected leading workforce planning and management practices for its IT workforce, we obtained and assessed documentation and compared it against the 15 selected practices. In particular, we analyzed the Secret Service's human capital strategic plan, human capital staffing plan, IT strategic plan, documentation of the component's staffing model that it used to determine the number of IT staff needed, an independent verification and validation report on the component's staffing models, documentation of the current number of IT staff, the Secret Service's

recruitment and outreach plans, documentation of DHS's hiring authorities (which are applicable to the Secret Service), the Secret Service's training strategic plan, IT workforce training plan, action plans for improving employee morale, and templates used for measuring and reporting employee performance.

We also interviewed Secret Service officials—including the CIO, Deputy CIO, and workforce planning staff—about the component's workforce-related policies and documentation. Further, we discussed with the officials the Secret Service's efforts to implement the selected workforce practices for its IT workforce.

Regarding our assessments of the Secret Service's implementation of the 15 selected workforce planning and management practices, we assessed a practice as being fully implemented if component officials provided supporting documentation that demonstrated all aspects of the practice. We assessed a practice as not implemented if the officials did not provide any supporting documentation for that practice, or if the documentation provided did not demonstrate any aspect of the practice. We assessed a practice as being partly implemented if the officials provided supporting documentation that demonstrated some, but not all, aspects of the selected practice.

In addition, related to our assessments of the Secret Service's implementation of the five selected overall workforce areas, we assessed each area as follows, based on the implementation of the three selected practices within each area:

- *Fully implemented:* The Secret Service provided evidence that it had fully implemented all three of the selected practices within the workforce area;
- *Substantially implemented:* The Secret Service provided evidence that it had either
  - fully implemented two selected practices and partly implemented the remaining one selected practice within the workforce area, or
  - fully implemented one selected practice and partly implemented the remaining two selected practices within the workforce area;
- *Partially implemented:* The Secret Service provided evidence that it had partly implemented each of the three selected practices within the workforce area;

- *Minimally implemented:* The Secret Service provided evidence that it had either
  - partly implemented two selected practices and not implemented the remaining one selected practice within the workforce area, or
  - partly implemented one selected practice and not implemented the remaining two selected practices within the workforce area; or
- *Not implemented:* The Secret Service did not provide evidence that it had implemented any of the three selected practices within the workforce area.

To address the third objective—determining the extent to which the Secret Service and DHS have implemented selected performance and progress monitoring practices for IITT—we reviewed leading project monitoring practices and guidance from the Software Engineering Institute. First, we reviewed the practices within the *Project Monitoring and Control* process area of the Institute's *Capability Maturity Model Integration® for Acquisition*.[20] Based on our review, we identified four practices associated with monitoring program performance and progress. In our professional judgment, all four of these practices were of significance to managing the IITT investment given the phase of the life cycle that the investment was in. As such, we elected to include all four of these practices in our review, and combined them into one practice, as follows:

- Monitor program performance and conduct reviews at predetermined checkpoints or milestones by, among other things, comparing actual cost, schedule, and performance data with estimates in the program plan and identifying significant deviations from established targets or thresholds for acceptable performance levels.

Next, given the agile development methodology that the Secret Service was using for certain projects within IITT,[21] we reviewed the Software Engineering Institute's technical note on the progress monitoring of agile

[20]Software Engineering Institute, *CMMI® for Acquisition, Version 1.3*, *Project Monitoring and Control* process area (Pittsburgh, PA: November 2010).

[21]Agile is a type of incremental development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach.

contractors.[22] Based on our review, and in consultation with an internal expert, we selected four agile metrics that the Institute identified as important for successful agile implementations and that, in our professional judgment, were of most significance to monitoring the performance of IITT's agile projects. We then combined these four metrics into one practice, as follows:

- Measure and monitor agile projects on velocity (i.e., number of story points completed per sprint or release), development progression (e.g., the number of features and user stories planned and accepted), product quality (e.g., number of defects), and post-deployment user satisfaction.

To determine the extent to which DHS and the Secret Service had implemented the first selected practice, we analyzed relevant program management and governance documentation for IITT's Enabling Capabilities program, and Multi-Level Security, Uniformed Division Resource Management System, and Events Management projects.[23] In particular, we analyzed acquisition program baselines, DHS acquisition decision event memorandums, artifacts from DHS and Secret Service program oversight reviews, cost monitoring reports, program integrated master schedules, and program status briefings, and compared this documentation to the selected practice. We also interviewed Secret Service OCIO officials regarding the Secret Service's and DHS's efforts to monitor the IITT investment's performance and progress.

To determine the extent to which the Secret Service had implemented the second selected practice related to measuring and monitoring agile projects on agile metrics (i.e., velocity, development progression, product quality, and post-deployment user satisfaction), we obtained and analyzed agile-related documentation for the two projects that the Secret Service was implementing using an agile methodology—Uniformed Division Resource Management System and Events Management. Specifically, to determine the extent to which the Secret Service was measuring and monitoring these two projects on metrics for velocity and

[22]Software Engineering Institute, *Agile Metrics: Progress Monitoring of Agile Contractors*, CMU/SEI-2013-TN-029 (January 2014).

[23]As previously discussed, Uniformed Division Resource Management System and Events Management were projects within the Enterprise Resource Management System program. The third project included in that program—called Enterprise-wide Scheduling—was still in the planning phase, as of June 2018. As such, we did not review it.

development progression, we obtained and analyzed documentation, such as sprint burndown charts and monthly program status reports, and compared it to the selected practice.

In addition, the agile metrics for product quality and post-deployment user satisfaction were only applicable to projects that had been deployed to users. As such, these metrics were applicable to the Uniformed Division Resource Management System (which the Secret Service had deployed to users) and were not applicable to Events Management (which the Secret Service had not yet deployed to users, as of early May 2018).

We therefore obtained and analyzed documentation demonstrating that Secret Service OCIO measured product defects for the Uniformed Division Resource Management System. We also requested documentation demonstrating that OCIO had measured and monitored post-deployment user satisfaction for this project, including via a survey. OCIO officials stated that they had not conducted such a survey and were unable to provide documentation demonstrating they had measured post-deployment user satisfaction for the Uniformed Division Resource Management System.

To assess the reliability of the cost, schedule, and agile-related data that were in DHS and the Secret Service's program management and governance documentation for the IITT investment, we (1) analyzed related documentation and assessed the data against existing agency records to identify consistency in the information, and (2) examined the data for obvious outliers, incomplete, or unusual entries. We determined that the data in these documents were sufficiently reliable for our purpose, which was to evaluate the extent to which DHS and the Secret Service had implemented processes for monitoring the IITT investment's performance and progress.

We conducted this performance audit from May 2017 to November 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Description of the U.S. Secret Service's Information Integration and Technology Transformation Investment's Programs and Projects

As of June 2018, the Secret Service's Information Integration and Technology Transformation (IITT) investment included two programs (one of which included three projects) and one project that had capabilities that were in planning or development and modernization, as described below:

- *Enabling Capabilities.* This program is intended to, among other things, (1) modernize and enhance the Secret Service's information technology (IT) network infrastructure, including increasing bandwidth and improving the speed and reliability of the Secret Service's IT system performance; (2) enhance cybersecurity to protect against potential intrusions and viruses; and (3) provide counterintelligence and data mining capabilities to improve officials' ability to perform the Secret Service's investigative mission.
- *Enterprise Resource Management System.* This program comprises three projects that are intended to provide:
  - a system that will enable the Secret Service's Uniformed Division to efficiently and effectively plan, provision, and schedule missions (this project is referred to as Uniformed Division Resource Management System),
  - a system that will unify the logistical actions (e.g., assigning personnel) surrounding special events that Secret Service agents need to protect, such as the United Nations General Assembly (this project is referred to as Events Management), and
  - a capability for creating schedules for Secret Service agents and administrative, professional, and technical staff, as well as the ability to generate reports on information such as monthly hours worked (this project is referred to as Enterprise-wide Scheduling).

- *Multi-Level Security.* This project is intended to enable authorized Secret Service users to view two levels of classified information on a single workstation. Previously, data at various security levels were contained and used in multiple disparate systems. Multi-Level Security is intended to streamline users' access to information at different security levels in order to enable them to more quickly and effectively perform their duties.

Table 15 provides the planned life cycle cost and schedule estimates (threshold values[1]) for each IITT program and project that had capabilities in planning or development and modernization, as of June 2018. In addition, the table describes any changes in those cost and schedule estimates, as well as the key reasons for any changes, as identified by officials from the Secret Service's Office of the Chief Information Officer.

Table 15: The U.S. Secret Service's Information Integration and Technology Transformation Investment's Programs and Projects That Had Capabilities in Planning or Development and Modernization, as of June 2018

Program/project name	Initial acquisition program baseline	Latest acquisition program baseline (or actual date)	Change in estimate	Key reasons for change, as identified by Secret Service officials
Enabling Capabilities program *(Initial baseline established in February 2011)*				
Life cycle cost estimate (then-year dollars in millions)	$712.7[a]	$622.5	↓ at least $90.2[b]	Decrease in scope and requirements following a significant schedule delay after a bid protest (discussed below). The removed requirements were either satisfied outside of the program or considered no longer necessary following the bid protest.
Initial operational capability[c]	3rd quarter FY 2014	April 2017[d]	→ 3 years	Bid protest led to the program awarding a new contract, which also resulted in changes to the development schedule.
Full operational capability[e]	Not identified	June 2018[d]	Unknown[f]	
Enterprise Resource Management System program[g]				

[1]A program's acquisition program baseline defines planned cost and schedule parameters in terms of an objective and minimum threshold value. According to DHS policy, if a program fails to meet any cost or schedule threshold approved in the acquisition program baseline, the program is considered to be in breach.

Program/project name	Initial acquisition program baseline	Latest acquisition program baseline (or actual date)	Change in estimate	Key reasons for change, as identified by Secret Service officials
Uniformed Division Resource Management System project *(Initial baseline established in April 2016)*				
Life cycle cost estimate (then-year dollars in millions)	$8.7	$12.9	↑ $4.2	Increases in (1) interface costs in order to address gaps in the selected solution and (2) operations and maintenance costs.
Initial operational capability	2nd quarter FY 2017	December 2016[d]	← 3 months	Use of an agile methodology and commercial off-the-shelf product solution.
Full operational capability	1st quarter FY 2018	May 2017[d]	← 7 months[h]	Use of an agile methodology and commercial off-the-shelf product solution.
Events Management project[l] *(Initial baseline established in April 2016)*				
Life cycle cost estimate (then-year dollars in millions)	$24.8	$24.3	↓ $0.5	Removal of certain operations and maintenance costs, in response to a budgetary directive that these costs not begin until the project's acquisition work has been completed.
Initial operational capability	2nd quarter FY 2019	May 2018[d]	← 10 months	Use of an agile methodology and commercial off-the-shelf product solution.
Full operational capability	1st quarter FY 2020	1st quarter FY 2020	None	
Enterprise-wide Scheduling project *(Initial baseline established in April 2016)*				
Life cycle cost estimate (then-year dollars in millions)	$8.1	$8.6	↑ $0.5	Additional program planning resulted in a better understanding of expected costs.
Initial operational capability	2nd quarter FY 2020	2nd quarter FY 2020	None	
Full operational capability	1st quarter FY 2021	1st quarter FY 2021	None	
Multi-Level Security project *(Initial baseline established in July 2013)*				
Life cycle cost estimate (then-year dollars in millions)	$30.6	$39.8	↑ $9.2	Increase in scope to (1) deliver additional workstations that are intended to use the multi-level security capability and (2) build secure rooms for processing classified information at Secret Service field offices.

Program/project name	Initial acquisition program baseline	Latest acquisition program baseline (or actual date)	Change in estimate	Key reasons for change, as identified by Secret Service officials
Initial operational capability	4th quarter FY 2013	December 2013[d]	→ 3 months	Administrative delay due to staffing availability for conducting acquisition decision event 3.
Full operational capability	3rd quarter FY 2016	4th quarter FY 2019	→ 3 years, 3 months	Technical delays in implementing requirements related to the use of federal identity verification cards.

Legend: FY = fiscal year; ↑ = cost increase; ↓ = cost decrease; → = schedule slippage; ← = schedule acceleration

Source: GAO analysis of U.S. Secret Service documentation and data reported by U.S. Secret Service officials. | GAO-19-60.

[a]Enabling Capabilities' initial acquisition program baseline did not include a life cycle cost estimate in then-year dollars (which would include the cost of inflation). Instead, this estimate is in budget year 2010 dollars and does not include the cost of inflation. As such, this estimate is less than what the estimate would be in then-year dollars.

[b]The estimate in Enabling Capabilities' initial acquisition program baseline was in budget year 2010 dollars and did not include the cost of inflation. If the estimate was in then-year dollars and included inflation, it would be higher. As such, the amount of the decrease in the estimate would also be greater.

[c]Initial operational capability is the point at which a subset of capabilities are first fielded to select users.

[d]These are actual dates.

[e]Full operational capability is the point at which an investment becomes fully operational.

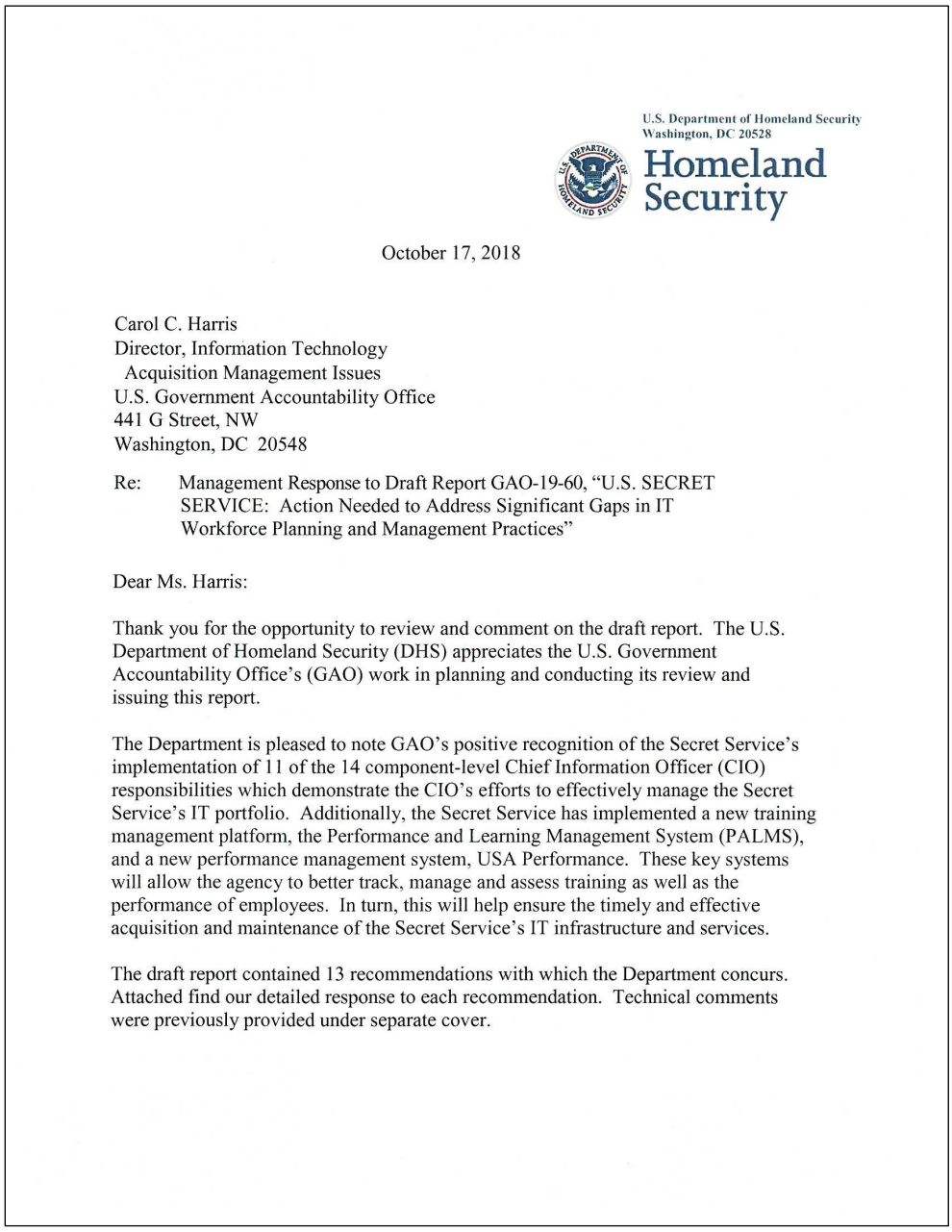
[f]The initial acquisition program baseline for Enabling Capabilities did not identify a planned date for full operational capability; as such, it is unknown whether or not the program has experienced a delay in achieving full operational capability.

[g]In addition to the life cycle costs for the Enterprise Resource Management System's projects, this program's life cycle costs also include about $22 million in sunk costs for the Combined Operations Logistics Database 2 program, which was the predecessor to the Enterprise Resource Management System. The Combined Operations Logistics Database 2 program began in 2009 and, after experiencing two schedule breaches and the program's contractor making insufficient progress in developing the system, in 2015 the Secret Service chose not to continue the contract. Subsequently, the Secret Service revised the program's acquisition approach and, in 2016, changed the program name to the Enterprise Resource Management System.

[h]While the Uniformed Division Resource Management System program reached full operational capability in May 2017—7 months ahead of the program's threshold date—Secret Service officials reported that they subsequently paused the phased rollout of the system due to operational performance issues with it. The officials stated that they worked with the vendor to address these issues and the final phased deployment of the system was in February 2018.

[i]In 2015, the Secret Service revised the acquisition approach for the Combined Operations Logistics Database 2 program—the predecessor to the Enterprise Resource Management System—to include the implementation of four projects. The Secret Service established an initial cost and schedule baseline for those four projects in April 2016. In February 2017, the Secret Service combined two of those four projects into the current project called Events Management (the remaining two projects—called Uniformed Division Resource Management System and Enterprise-wide Scheduling—did not change). The initial life cycle cost estimate listed for Events Management reflects the baseline costs established in April 2016 for the two projects that were combined into Events Management.

Appendix III: Comments from the Department of Homeland Security



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

Homeland Security

October 17, 2018

Carol C. Harris
Director, Information Technology
Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-60, "U.S. SECRET SERVICE: Action Needed to Address Significant Gaps in IT Workforce Planning and Management Practices"

Dear Ms. Harris:

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

The Department is pleased to note GAO's positive recognition of the Secret Service's implementation of 11 of the 14 component-level Chief Information Officer (CIO) responsibilities which demonstrate the CIO's efforts to effectively manage the Secret Service's IT portfolio. Additionally, the Secret Service has implemented a new training management platform, the Performance and Learning Management System (PALMS), and a new performance management system, USA Performance. These key systems will allow the agency to better track, manage and assess training as well as the performance of employees. In turn, this will help ensure the timely and effective acquisition and maintenance of the Secret Service's IT infrastructure and services.

The draft report contained 13 recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

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

Sincerely,

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

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-19-60

GAO recommended that the Director of the Secret Service:

Recommendation 1: Ensure that the CIO establishes and documents an IT acquisition review process that ensures that the CIO or the CIO's delegate reviews all contracts containing IT, as appropriate.

Response: Concur. The Secret Service's CIO has updated policy directive, CIO 01(03) "IT Purchase," with additional guidance to ensure the policy reflects that all IT purchases must go through the CIO's office for approval. The CIO IT Governance office will work with the Secret Service Office of the Chief Financial Officer's Procurement Division to identify IT contracts and procurements so they are appropriately routed to the CIO for approval in the procurement system. Estimated Completion Date (ECD): October 31, 2019.

Recommendation 2: Update the enterprise governance policy to specify (1) the CIO's current role and responsibilities on the Executive Resources Board, to include developing and reviewing the IT budget formulation and execution, and (2) the Deputy CIO's (DCIO) role and responsibilities on the Enterprise Governance Council.

Response: Concur. The Secret Service Office of Strategic Planning and Policy (OSP) is updating its enterprise governance policy and related policies, which will outline the CIO and DCIO's roles and responsibilities, as well as those of other Assistant Directors, Executive Chiefs, Deputy Assistant Directors, and Deputy Chiefs. ECD: March 31, 2019.

Recommendation 3: Ensure that the Secret Service develops a charter for its Executive Resources Board that specifies the roles and responsibilities of all Board members, including the CIO.

Response: Concur. The OSP began developing an Executive Resources Board (ERB) charter in February of 2018. The ERB is currently comprised of six Assistant Directors and six Executive Chiefs, including the CIO. The Secret Service does not have plans to add members to the ERB at this time. The roles and responsibilities of ERB members will also be addressed in Secret Service's charter. ECD: March 31, 2019.

Recommendation 4: Ensure that the CIO includes product quality and post-deployment user satisfaction metrics in the modular outcomes and target measures that the CIO sets for monitoring agile projects.

3

Response: Concur. The Secret Service will include a post-deployment user satisfaction survey for all future programs, projects and services delivered from the Secret Service's Office of the Chief Information Officer (OCIO). More specifically, the Secret Service will comply with DHS Guidebook, 102-01-103-01, "Systems Engineering Life Cycle Guidebook" (SELC) and include a post-implementation review for projects within 6 - 18 months of achieving initial operational capability. Furthermore, as required in both the SELC and Capital Planning and Investment Control processes, an annual Operational Analysis (OA) will be conducted. The OA requirement in the SELC Guidebook includes a number of different deployment measures of performance. One such measure is a user satisfaction survey which is planned for one of the projects evaluated in the GAO's report. ECD: October 31, 2019.

Recommendation 5: Ensure that the CIO identifies all of the required knowledge and skills for the IT workforce.

Response: Concur. The OCIO will continue to identify any training gaps or needs and conduct remediation training as appropriate. As new technology is deployed the OCIO training coordinator will work with senior management and subject matter experts to develop up-front training requirements and schedule training as required. This process will be documented in an OCIO standard operating procedure for training. ECD: March 31, 2019.

Recommendation 6: Ensure that the CIO regularly analyzes the IT workforce to identify its competency needs and any gaps it may have.

Response: Concur. The Secret Service has participated in the DHS working group that was formed to address GAO High Risk Audit ITM 4 – "IT Human Capital Management" and will utilize the requisite competency models produced from this analysis to begin a process of regularly analyzing the IT workforce with the goal of:

- Assessing overall workforce health and providing recommendations for areas of improvement;
- Employing a more manageable, phased approach, dividing the IT Workforce into four functional area groups for the assessment;
- Developing recommendations to support career growth and development;
- Crafting actionable talent management and training solutions;
- Leveraging relevant, authoritative products like the National Institute of Standards and Technology Cybersecurity Workforce Framework to deliver a "Best in Class" solution; and
- Participating in an ongoing DHS review of the requirements for IT Project Management training certification.

4

ECD: October 31, 2019.

Recommendation 7: Ensure that after OCIO completes an analysis of the IT workforce to identify any competency and staffing gaps it may have, the Secret Service updates its recruiting and hiring strategies and plans to address those gaps, as necessary.

Response: Concur. The Secret Service's Office of Human Resources' (HUM) Outreach Branch (ORB) will continue to partner with the OCIO and the DHS Office of Academic Engagement (OAE) to identify universities, colleges and other locations with STEM/CYBER, computer science, software/ computer engineering, information technology, network engineering curricula where students acquire the skill sets and requisite qualifications that are essential to IT professionals. Targeted visits to these universities will foster relationships with career placement professionals who can direct students seeking employment to Secret Service recruiters and field office personnel.

OAE also collaborates with the DHS Homeland Security Academic Advisory Council (HSAAC). The HSAAC is a Federal advisory committee comprised of university and college presidents, academic leaders, and interagency partners. Through the HSAAC's network, OAE can conduct tailored outreach to more than 2,500 institutions of higher education. The Secret Service will continue to work with these entities and others such as the National Association of Colleges and Employers, the Higher Education Association and the five Minority Serving Institutions to market career opportunities within the Secret Service.

The ORB regularly researches career fairs, conferences, symposiums and networking events to identify and recruit qualified persons with appropriate certifications for the 2210 and 0391 series positions. Emphasis will be placed on STEM/CYBER related conferences and institutions by developing partnerships with corporate entities with a proven track record in bringing top STEM/CYBER candidates to IT/STEM/CYBER hiring events.

Additionally, the ORB will continue to leverage the Cyber Direct Hiring Authority while establishing and enhancing recruiting partnerships with the top 22 STEM/CYBER educational institutions in the U.S. Partnerships with corporate entities with a proven track record in bringing top STEM/CYBER candidates to IT/STEM/CYBER hiring events for us to market our brand and career opportunities. Additionally, the Secret Service will prioritize usage of the Veterans Recruitment Appointment and leverage the Veteran's Database to identify individuals with the knowledge, skills and abilities applicable within OCIO's program offices. ECD: October 31, 2019.

Recommendation 8: Ensure that the Office of Human Resources (1) develops and tracks metrics to monitor the effectiveness of the Secret Service's recruitment activities for the IT workforce, including their effectiveness at addressing skill and staffing gaps; and (2) reports to component leadership on those metrics.

5

Response: Concur. HUM seeks to improve its tracking metrics to monitor the effectiveness of the agency's recruitment activities. The ORB is continuously identifying and adopting best practices to engage their target audience and address the agency's needs thus maximizing the return on investment. As such, the Branch provides data to the Department monthly regarding metrics on recruitment efforts towards designated Priority Mission Critical Occupations. Secret Service and DHS leadership use these metrics to guide recruitment efforts. The IT workforce as well as other specific mission critical support positions (e.g. procurement, financial management) are also included in these statistics. Additionally, Secret Service's Workforce Planning Division tracks all CIO hiring activities with information received from National Finance Center on a bi-weekly basis that includes the job series and title, as well as other relevant position characteristics. This information is compared to staffing data with CIO position allocation information to monitor positions filled against those that remain vacant. HUM meets weekly with the agency's Deputy Director and Chief Operating Officer to ensure emphasis is focused on those critical positions such as cyber.

The ORB recently initiated its FY 2019 recruitment strategy to include sourcing cyber/ STEM resumes and inviting a representative from the OCIO team to recruitment and hiring events when appropriate. For example, on October 9, 2018 the Cyber Maryland hiring fair was attended by members of both the OCIO and ORB. This event was targeted to support the Cyber/ STEM program. More than 50 resumes were collected on site along with access to all resumes of over 400 registered participants. The OCIO will be conducting interviews of strong candidates as a result of the event.

The disposition of the candidates will be tracked for future use to weigh the effectiveness of the recruiting efforts. Prior to this event, 150 resumes from Pre-registrants were received. The OCIO identified 16 individuals that met their criteria and selected five names of registrants they contacted. ECD: October 31, 2019.

Recommendation 9: Ensure that the Office of Human Resources and OCIO adjust their recruitment and hiring plans and activities, as necessary, after establishing and tracking metrics for assessing the effectiveness of these activities for the IT workforce.

Response: Concur. HUM will monitor monthly the established metrics as it relates to the effectiveness of the recruitment and onboarding activities. Data reflecting the Cyber /STEM program will be utilized to provide the agency leadership an opportunity to implement course adjustments throughout the year. Additionally, HUM's weekly staffing meetings with the CIO will afford the opportunity to identify opportunities for improvement and evaluate the effectiveness of initiatives. ECD: October 31, 2019.

6

Recommendation 10: Ensure that the CIO (1) defines the required training for each IT workforce group, (2) determines the activities that OCIO will include in its IT workforce training and development program based on its available training budget, and (3) implements those activities.

Response: Concur. The Secret Service OCIO recently developed training requirements for each workforce group, which was issued during GAO's audit fieldwork. In FY 2019, the OCIO began exploring options to deliver this training to all of the workforce within the current budget constraints. ECD: October 31, 2019.

Recommendation 11: Ensure that the CIO ensures that the IT workforce completes training specific to their positions (after defining the training required for each workforce group).

Response: Concur. The Secret Service Office of Training implemented PALMS in the third quarter of FY 2018 to track employees' training. In FY 2019, the OCIO will implement virtual training by utilizing Safari Books' online learning and training platform. This resource will allow our training manager to implement training paths for each workforce group as well as provide access to a host of thousands of online-training resources as well as live classes. Additionally, by using this capability Secret Service managers can develop training specific to positions and workgroups. ECD: October 31, 2019.

Recommendation 12: Ensure that the CIO collects and assesses performance data (including qualitative or quantitative measures, as appropriate) to determine how the IT training program contributes to improved performance and results (once the training program is implemented).

Response: Concur. The Secret Service will utilize all virtual training resources at its disposal to address this recommendation, as appropriate, including PALMS and Safari Books. OCIO will begin tracking in more detail any post-training assessments administered to employees and develop an in-house valuation process to measure improved performance based on completed training. ECD: March 31, 2019.

Recommendation 13: Ensure that the CIO updates the performance plans for each occupational series within the IT workforce to include the relevant technical competencies, once identified, against which IT staff performance should be assessed.

Response: Concur. The Secret Service's use of USA Performance allows the OCIO to include the relevant technical competencies as appropriate in the future. The OCIO will use this feature in the next performance cycle beginning in July 2019. ECD: July 31, 2019.

7

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Shannin O'Neill (Assistant Director), Emily Kuhn (Analyst-in-Charge), Quintin Dorsey, Rebecca Eyler, Javier Irizarry, and Paige Teigen.

Appendix V: Accessible Data

Agency Comment Letter

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

Page 1

October 17, 2018

Carol C. Harris
Director, Information Technology
Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-60, "U.S. SECRET SERVICE: Action Needed to Address Significant Gaps in IT Workforce Planning and Management Practices"

Dear Ms. Harris:

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

The Department is pleased to note GAO's positive recognition of the Secret Service's implementation of 11 of the 14 component-level Chief Information Officer (CIO) responsibilities which demonstrate the CIO's efforts to effectively manage the Secret Service's IT portfolio. Additionally, the Secret Service has implemented a new training management platfom1, the Perfom1ance and Learning Management System (PALMS), and a new performance management system, USA Performance. These key systems will a1low the agency to better track, manage and assess training as well as the perfom1ance of employees. In turn, this will help ensure the timely and effective acquisition and maintenance of the Secret Service's IT infrastructure and services.

The draft report contained 13 recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Page 2

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

Sincerely,

Jim H. Crumpacker, CIA, CFE
Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GAO-19-60

GAO recommended that the Director of the Secret Service:

Recommendation 1:

Ensure that the CIO establishes and documents an IT acquisition review process that ensures that the CIO or the CIO's delegate reviews all contracts containing IT, as appropriate.

Response: Concur. The Secret Service's CIO has updated policy directive, CIO 01(03) "IT Purchase," with additional guidance to ensure the policy reflects that all IT purchases must go through the CIO's office for approval. The CIO IT Governance office will work with the Secret Service Office of the Chief Financial Officer's Procurement Division to identify IT contracts and procurements so they are appropriately routed to the CIO for approval in the procurement system. Estimated Completion Date (ECD): October 31, 2019.

Recommendation 2:

Update the enterprise governance policy to specify (1) the CIO's current role and responsibilities on the Executive Resources Board, to include developing and reviewing the IT budget formulation and execution, and (2) the Deputy CIO's (DCIO) role and responsibilities on the Enterprise Governance Council.

Response: Concur. The Secret Service Office of Strategic Planning and Policy (OSP) is updating its enterprise governance policy and related policies, which will outline the CIO and DCIO's roles and responsibilities, as well as those of other Assistant Directors, Executive Chiefs, Deputy Assistant Directors, and Deputy Chiefs. ECD: March 31, 2019.

Recommendation 3:

Ensure that the Secret Service develops a charter for its Executive Resources Board that specifies the roles and responsibilities of all Board members, including the CIO.

Response: Concur. The OSP began developing an Executive Resources Board (ERB) charter in February of 2018. The ERB is currently comprised of six Assistant Directors and six Executive Chiefs, including the CIO. The Secret Service does not have plans to add members to the ERB at this time. The roles and responsibilities of ERB members will also be addressed in Secret Service' s charter. ECD: March 31, 2019.

Recommendation 4:

Ensure that the CIO includes product quality and post- deployment user satisfaction metrics in the modular outcomes and target measures that the CIO sets for monitoring agile projects.

Page 4

Response: Concur. The Secret Service will include a post-deployment user satisfaction survey for all future programs, projects and services delivered from the Secret Service's Office of the Chief Information Officer (OCIO). More specifically, the Secret Service will comply with DHS Guidebook, 102-01-103-01, "Systems Engineering Life Cycle Guidebook" (SELC) and include a post-implementation review for projects within 6 - 18 months of achieving initial operational capability. Furthermore, as required in both the SELC and Capital Planning and Investment Control

processes, an annual Operational Analysis (OA) will be conducted. The OA requirement in the SELC Guidebook includes a number of different deployment measures of performance. One such measure is a user satisfaction survey which is planned for one of the projects evaluated in the GAO's report. ECD: October 31, 2019.

Recommendation 5:

Ensure that the CIO identifies all of the required knowledge and skills for the IT workforce.

Response: Concur. The OCIO will continue to identify any training gaps or needs and conduct remediation training as appropriate. As new technology is deployed the OCIO training coordinator will work with senior management and subject matter experts to develop up-front training requirements and schedule training as required. This process will be documented in an OCIO standard operating procedure for training. ECD: March 31, 2019.

Recommendation 6:

Ensure that the CIO regularly analyzes the IT workforce to identify its competency needs and any gaps it may have.

Response: Concur. The Secret Service has participated in the DHS working group that was formed to address GAO High Risk Audit ITM 4 - "IT Human Capital Management" and will utilize the requisite competency models produced from this analysis to begin a process of regularly analyzing the IT workforce with the goal of:

- Assessing overall workforce health and providing recommendations for areas of improvement;
- Employing a more manageable, phased approach, dividing the IT Workforce into four functional area groups for the assessment;
- Developing recommendations to support career growth and development;
- Crafting actionable talent management and training solutions;
- Leveraging relevant, authoritative products like the National Institute of Standards and Technology Cybersecurity Workforce Framework to deliver a "Best in Class" solution; and

- Participating in an ongoing DHS review of the requirements for IT Project Management training certification.

Page 5

ECD: October 31, 2019.

Recommendation 7:

Ensure that after OCIO completes an analysis of the IT workforce to identify any competency and staffing gaps it may have, the Secret Service updates its recruiting and hiring strategies and plans to address those gaps, as necessary.

Response: Concur. The Secret Service's Office of Human Resources' (HUM) Outreach Branch (ORB) will continue to partner with the OCIO and the DHS Office of Academic Engagement (OAE) to identify universities, colleges and other locations with STEM/CYBER, computer science, software/ computer engineering, information technology, network engineering curricula where students acquire the skill sets and requisite qualifications that are essential to IT professionals. Targeted visits to these universities will foster relationships with career placement professionals who can direct students seeking employment to Secret Service recruiters and field office personnel.

OAE also collaborates with the DHS Homeland Security Academic Advisory Council (HSAAC). The HSAAC is a Federal advisory committee comprised of university and college presidents, academic leaders, and interagency partners. Through the HSAAC's network, OAE can conduct tailored outreach to more than 2,500 institutions of higher education. The Secret Service will continue to work with these entities and others such as the National Association of Colleges and Employers, the Higher Education Association and the five Minority Serving Institutions to market career opportunities within the Secret Service.

The ORB regularly researches career fairs, conferences, symposiums and networking events to identify and recruit qualified persons with appropriate certifications for the 2210 and 0391 series positions. Emphasis will be placed on STEM/CYBER related conferences and institutions by developing partnerships with corporate entities with a proven track record in bringing top STEM/CYBER candidates to IT/STEM/CYBER hiring events .

Additionally, the ORB will continue to leverage the Cyber Direct Hiring Authority while establishing and enhancing recruiting partnerships with the top 22 STEM/CYBER educational institutions in the U.S. Partnerships with corporate entities with a proven track record in bringing top STEM/CYBER candidates to IT/STEM/CYBER hiring events for us to market our brand and career opportunities. Additionally, the Secret Service will prioritize usage of the Veterans Recruitment Appointment and leverage the Veteran's Database to identify individuals with the knowledge, skills and abilities applicable within OCIO's program offices. ECD: October 31, 2019.

Recommendation 8:

Ensure that the Office of Human Resources (1) develops and tracks metrics to monitor the effectiveness of the Secret Service's recruitment activities for the IT workforce, including their effectiveness at addressing skill and staffing gaps; and (2) reports to component leadership on those metrics.

Page 6

Response: Concur. HUM seeks to improve its tracking metrics to monitor the effectiveness of the agency's recruitment activities. The ORB is continuously identifying and adopting best practices to engage their target audience and address the agency's needs thus maximizing the return on investment. As such, the Branch provides data to the Department monthly regarding metrics on recruitment efforts towards designated Priority Mission Critical Occupations. Secret Service and DHS leadership use these metrics to guide recruitment efforts. The IT workforce as well as other specific mission critical support positions (e.g. procurement, financial management) are also included in these statistics. Additionally, Secret Service's Workforce Planning Division tracks all CIO hiring activities with information received from National Finance Center on a bi-weekly basis that includes the job series and title, as well as other relevant position characteristics. This information is compared to staffing data with CIO position allocation information to monitor positions filled against those that remain vacant. HUM meets weekly with the agency's Deputy Director and Chief Operating Officer to ensure emphasis is focused on those critical positions such as cyber.

The ORB recently initiated its FY 2019 recruitment strategy to include sourcing cyber/ STEM resumes and inviting a representative from the OCIO team to recruitment and hiring events when appropriate. For

example, on October 9, 2018 the Cyber Maryland hiring fair was attended by members of both the OCIO and ORB. This event was targeted to support the Cyber/ STEM program. More than 50 resumes were collected on site along with access to all resumes of over 400 registered participants. The OCIO will be conducting interviews of strong candidates as a result of the event.

The disposition of the candidates will be tracked for future use to weigh the effectiveness of the recruiting efforts. Prior to this event, 150 resumes from Pre- registrants were received. The OCIO identified 16 individuals that met their criteria and selected five names of registrants they contacted. ECD: October 31, 2019.

Recommendation 9:

Ensure that the Office of Human Resources and OCIO adjust their recruitment and hiring plans and activities, as necessary, after establishing and tracking metrics for assessing the effectiveness of these activities for the IT workforce.

Response: Concur. HUM will monitor monthly the established metrics as it relates to the effectiveness of the recruitment and onboarding activities. Data reflecting the Cyber /STEM program will be utilized to provide the agency leadership an opportunity to implement course adjustments throughout the year. Additionally, HUM's weekly staffing meetings with the CIO will afford the opportunity to identify opportunities for improvement and evaluate the effectiveness of initiatives. ECD: October 31, 2019.

Page 7

Recommendation 10:

Ensure that the CIO (1) defines the required training for each IT workforce group, (2) determines the activities that OCIO will include in its IT workforce training and development program based on its available training budget, and (3) implements those activities.

Response: Concur. The Secret Service OCIO recently developed training requirements for each workforce group, which was issued during GAO's audit fieldwork. In FY 2019, the OCIO began exploring options to deliver this training to all of the workforce within the current budget constraints. ECD: October 31, 2019.

Recommendation 11:

Ensure that the CIO ensures that the IT workforce completes training specific to their positions (after defining the training required for each workforce group).

Response: Concur. The Secret Service Office of Training implemented PALMS in the third quarter of FY 2018 to track employees' training. In FY 2019, the OCIO will implement virtual training by utilizing Safari Books' online learning and training platform. This resource will allow our training manager to implement training paths for each workforce group as well as provide access to a host of thousands of online- training resources as well as live classes. Additionally, by using this capability Secret Service managers can develop training specific to positions and workgroups. ECD: October 31, 2019.

Recommendation 12:

Ensure that the CIO collects and assesses performance data (including qualitative or quantitative measures, as appropriate) to determine how the IT training program contributes to improved performance and results (once the training program is implemented).

Response: Concur. The Secret Service will utilize all virtual training resources at its disposal to address this recommendation, as appropriate, including PALMS and Safari Books. OCIO will begin tracking in more detail any post-training assessments administered to employees and develop an in-house valuation process to measure improved perfom1ance based on completed training. ECD: March 31, 2019.

Recommendation 13:

Ensure that the CIO updates the performance plans for each occupational series within the IT workforce to include the relevant technical competencies, once identified, against which IT staff perf01mance should be assessed.

Response: Concur. The Secret Service's use of USA Performance allows the OCIO to include the relevant technical competencies as appropriate in the future. The OCIO will use this feature in the next performance cycle beginning in July 2019. ECD: July31, 2019.

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 (https://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 https://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, https://www.gao.gov/ordering.htm.

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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