



Audit of the Bureau of Alcohol, Tobacco, Firearms
and Explosives' Enterprise Standard Architecture V
Task Order Awarded to Leidos, Inc.



AUDIT DIVISION

23-103

SEPTEMBER 2023



EXECUTIVE SUMMARY

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Enterprise Standard Architecture V Task Order Awarded to Leidos, Inc.

Objectives

The Department of Justice (DOJ) Office of the Inspector General (OIG) conducted an audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Enterprise Standard Architecture (ESA) V task order for information technology (IT) services. The objectives of our audit were to assess: (1) ATF's acquisition planning and selection of Leidos, Inc. (Leidos) for the ESA V task order awarded; (2) ATF's administration and oversight of the task order; and (3) Leidos' performance on the task order, including financial management, monitoring, reporting, and progress towards meeting the task order goals and objectives.

Results in Brief

The DOJ OIG completed an audit of ATF's ESA V task order awarded to Leidos. Awarded in May 2020, this 9-year task order was available to all DOJ components and other federal agencies (collectively termed federal components). We found that ATF adequately justified its selection of Leidos and generally performed the appropriate administration and oversight of the task order. However, the task order's Key Performance Indicators (KPI) did not always contain effective disincentives, or lacked disincentives to ensure Leidos' performance met the federal components' standards. Further, we found instances where the task order could have been structured differently to better meet the federal components' needs. These issues and added projects contributed to the task order costs increasing 85 percent since the May 2020 award. Further, federal components expressed dissatisfaction with Leidos' work performance and delays in getting work accomplished due to Leidos contesting that work assigned was outside the scope of task order. These delays left risks to government IT systems insufficiently mitigated within required timeframes.

Recommendations

We identified 8 recommendations for ATF to improve the management of its ESA V task order, which will help improve oversight of contractor performance and facilitate contractor accountability. ATF concurred with 5 of our recommendations and partially concurred with the remaining 3 recommendations. Leidos and ATF's responses are contained within in Appendix 4 and 5, respectively. Our analysis of those responses is included in Appendix 6.

Audit Results

During this contract, Leidos was responsible to provide support to participating federal components for 12 IT services, including services for account management and directory, application hosting, and monitoring and management.

ATF's Acquisition Planning and Ongoing Contract Management

Based on our evaluation of the ESA V contract file, we concluded that ATF adequately justified the award to Leidos. ATF also generally performed the appropriate administration and oversight of the task order, and the federal components participating in the ESA V program spoke highly of the responsiveness of ATF's contracting team.

ATF Should Utilize More Effective Key Performance Indicators

Our evaluation of the task order's Quality Assurance Surveillance Plan determined that the KPI did not always contain effective disincentives, allowing for the Government to withhold a portion of payment for nonperformance of contract requirements, such as security patching and print services. Specifically, there were no disincentives for 20 of the 51 KPIs (39 percent). Additionally, some federal components told us they did not agree with Leidos' monthly status reports, in which

Leidos indicated they had met the performance standards. For example, ATF stated that Leidos did not meet the standards for timely installation of IT security patches, which are critical in mitigating risk of system breaches. However, ATF did not utilize disincentives for Leidos not meeting these deadlines. Finally, ATF also did not retain documentation on how the performance standards were developed, and ATF had not reevaluated the standards since the task order award, even after they proved ineffective in improving contractor performance.

ATF Should Better Engage Participating Federal Components

ATF did not address concerns from a federal component regarding use of a fixed price contract structure prior to awarding the task order. We believe the use of a fixed price structure for some services under the task order has reduced flexibility and contributed to scope contentions and escalating costs for some components. For example, after Justice Management Division (JMD) was informed by Leidos that several contract staff were being replaced with lesser qualified workers under their current fixed price project, JMD modified its order with Leidos, allowing the experienced contract workers to remain on the contract. This resulted in JMD allocating additional, unbudgeted funds to maintain the same level of service.

The federal components and Leidos had disagreements over the scope of work due to different interpretations of Performance Work Statement (PWS). We found that these scope contentions unnecessarily delayed some projects, which were later determined to be within scope. As a result, the Government drafted six Letters of Concern, formally issuing three to Leidos, to assist in resolving scope contentions and performance concerns.

Leidos Should Meet Security Patch Deadlines and Submit Accurate Monthly Reporting

On November 5, 2021, ATF provided Leidos a list of security patches that required remediation before dates ranging from November 17 through December 1, 2021. Leidos stated that, although the applications of patches were within the scope of the task order, to meet the timelines additional staff would be needed at an additional cost to the Government. According to the November 30, 2021, Security Posture Dashboard Report (SPDR) from the Department Office of the Chief Information Officer (OCIO), unaddressed cyber vulnerabilities affected 980 devices. The contracting

officer issued a letter of concern on December 20, 2021, to document Leidos' unwillingness to perform the in-scope work. By January 11, 2022, the number of devices not fully updated with the necessary security patches had reduced to 118 devices and on February 8, 2022, ATF officially closed the Letter of Concern, agreeing with Leidos' corrective actions. As this example demonstrates, scope contentions can lead to missed deadlines, which in this case resulted in unmitigated risks to known security vulnerabilities.

The ESA V task order's PWS requires Leidos to provide federal components with monthly status reports that contain compliance levels, management and technical progress, and challenges. However, we found that Leidos' monthly status reports were not accurate and did not identify challenges and contentions regarding the security patches at that time.

ATF Should Update its Procedures for Documenting Security Patching

ATF's standard operating procedures on security patches stated that reports would be available to track individual cyber vulnerabilities from inception to completion. ATF stated that it is no longer using those reports and has not updated its procedures. Instead, ATF uses the SPDR from the Department's OCIO to track security patch installation. However, the SPDR is a snapshot of active vulnerabilities identified, and ATF could not provide us with historical reports demonstrating the timely remediation of vulnerabilities.

ATF Should Perform Forecasting and Risk Assessments to Determine Impact of Changing Participation

The purpose of the ESA V task order was to maximize the usage of contractor-provided managed services for the Government's IT services and help the Government save money over time through shared services that provide economies of scale. However, changes in program participation affected the cost distribution to the remaining federal components. Leidos did not achieve the costs savings it anticipated and submitted a modified cost proposal to ATF's contracting officer. Leidos' pricing proposal did not discuss the potential price changes when other federal components leave the program. Also, ATF did not assess the risk of federal components descopeing or withdrawing from the program. The increased costs may negatively impact agencies' budgets as agencies would have to allocate additional money for ESA V services for which they had not planned.

Table of Contents

Introduction	1
History of ATF's Enterprise Standard Architecture Task Order.....	1
ATF's Management of the ESA V Task Order	1
Task Order Requirements for ATF and Other Federal Components.....	2
Office of the Inspector General Audit Approach.....	3
Audit Results	5
ATF's Acquisition Planning and Ongoing Contract Management was Appropriate	5
ATF Should Utilize More Effective Key Performance Indicators.....	5
ATF Should Better Engage Participating Federal Components	8
JMD Expressed Concerns About Contract Cost Model Prior to Award	8
Performance Work Statements Should be Better Aligned and Documented to Avoid Scope Disagreements.....	9
Leidos Should Meet Security Patch Deadlines and Submit Accurate Monthly Reporting.....	12
Meeting Deadlines on Security Patch Installations.....	13
Monthly Reports that Discuss Progress and Challenges	13
ATF Should Update its Procedures for Documenting Security Patching	14
ATF Should Perform Forecasting and Risk Assessments to Determine Impact of Changing Participation	15
Conclusion and Recommendations	18
APPENDIX 1: Objectives, Scope, and Methodology	20
Objectives	20
Scope and Methodology.....	20
Statement on Compliance with Generally Accepted Government Auditing Standards	20
Internal Controls.....	21
Compliance with Laws and Regulations	21
Sample-Based Testing.....	22
Computer-Processed Data	22
APPENDIX 2: ESA V CLIN Descriptions	23
APPENDIX 3: Federal Components' Task Order Descriptions	26
APPENDIX 4: Leidos, Inc.'s Response to the Draft Audit Report	29
APPENDIX 5: The Bureau of Alcohol, Tobacco, Firearms and Explosives' Response to the Draft Audit Report	31

APPENDIX 6: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report..... 35

Introduction

The Department of Justice (DOJ) Office of the Inspector General (OIG) completed an audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Enterprise Standard Architecture (ESA) V task order awarded to Leidos, Inc. (Leidos). Awarded in May 2020, the ESA V task order was valued at \$492.7 million and had a 9-year period of performance of May 1, 2020, through April 30, 2029.¹ The purpose of this task order is to provide service-oriented information technology (IT) support to all DOJ components and other federal Government agencies, collectively termed "federal components." The ESA V task order is intended to serve the federal components' IT needs through core services that provide a highly secure, cost-effective, performance-based, innovation-minded service environment for the federal components that can be incrementally transitioned to a Contractor-owned and -managed shared environment.

The ESA V task order was awarded under the General Services Administration (GSA) Government Wide Award Contract (GWAC) called Alliant II.² The Alliant II GWAC is a multiple-award, indefinite delivery, indefinite-quantity contract offering IT solutions under various contract types, including fixed price, cost reimbursement, labor hours, time and materials (T&M), and hybrids.

History of ATF's Enterprise Standard Architecture Task Order

ATF first started its ESA program in the mid 1990s, serving only its IT needs. In 2004, during ESA III, US Marshall participated in the ESA program and the department began to consider the idea of enterprise contracts across the Government. According to ATF's Chief Information Officer (CIO), the Department of Justice CIO and former ATF CIO encouraged procurement offices to establish enterprise contracts that would benefit the entire department through economies of scale. Thus, beginning with ESA IV, more DOJ components started to participate in the task order. In December 2012, ATF solicited the Alliant contract and awarded the ESA IV to a different contractor, which in 2016 was merged with Leidos.

In August 2019, ATF again solicited GSA's Alliant II GWAC to service its ESA V task order and awarded the task order to Leidos. ATF made the ESA V task order available to federal components within the DOJ as well as agencies outside of the DOJ.

ATF's Management of the ESA V Task Order

The ESA V task order was awarded by ATF's Office of Management, Property, Acquisitions and Safety Divisions' Acquisition Branch. The ESA V task order is administered by a contracting officer and four contracting officer representatives (COR) who assist in monitoring the contractor's performance and performing other contract administration duties.

¹ ESA V was the fifth iteration of ATF's ESA program.

² A GWAC is a pre-competed, multiple-award, indefinite delivery, indefinite quantity contract that agencies can award against. The GSA Alliant II is a GWAC with 44 contractors offering complete and flexible IT solutions. Alliant II has a contract ceiling of \$50 Billion and a period of performance of July 1, 2018, through June 30, 2023, plus one five-year option from July 1, 2023, to June 30, 2028. The Alliant II supports all contract types: fixed price, cost reimbursement, labor hour, time and materials and hybrids. GSA charges a Contract Access Fee of 0.75 percent to utilize this GWAC.

The primary client organization for the ESA V program is ATF's Office of Science and Technology, which is led by ATF's CIO. Other federal components subscribing to the ESA program have assigned task managers, who are responsible for reviewing invoices, attending meetings with Leidos, and providing monthly feedback on Leidos' performance to ATF's contracting team.

Although the Justice Management Division's (JMD) Procurement Services Staff (PSS) office awards and manages large department-wide contracts, the PSS Assistant Director informed us that they did not have the capacity to manage a contract of this magnitude. JMD also acknowledged that it would charge DOJ components a contract management fee for similar contract services they subscribe to, while ATF currently does not charge the ESA V federal components a fee for managing the task order. ATF's CIO informed us that the associated operational overhead is not significant and would be too burdensome to isolate and calculate passthrough costs to charge other federal components supported with the ESA V program.

Task Order Requirements for ATF and Other Federal Components

At the end of ESA IV, ATF hired the services of an outside consultant to help with the acquisition process of ESA V, including the acquisition planning process, writing the performance work statement (PWS), and the bid evaluation process. The PWS contains 14 separate contract line item numbers (CLIN), which define the contract deliverables, contract type, places of performance, total price, and funding source.³ The CLINs are used to organize the various services the Government needs. Each CLIN in ESA V was additionally assigned a specific billing structure, such as Fixed Unit Rate (FUR), T&M, or Firm Fixed Price (FFP). Each participating federal component reviewed the task order's base PWS, determined CLINs to which it would subscribe, and provided the contracting officer any needed supplemental requirements. However, the federal components could not change the billing structure of the CLINs (i.e., T&M or FFP), as they were pre-determined by ATF. We summarized the general task order requirements by CLIN in Appendix 2 and federal component specific requirements in Appendix 3. Table 1 below depicts the ATF, Drug Enforcement Administration's (DEA), United States Trustee Program (USTP), Antitrust Division (ATR) General Support System (GSS) and Management System Staff (MSS), JMD, and OIG's subscribed services at the time of the ESA V task order award.

³ Federal Acquisition Regulation 4.1001(a) states, "Line items are established to define deliverables or organize information about deliverables. Each line item describes characteristics for the item purchased, e.g., pricing, delivery, and funding information."

Table 1

Federal Components Task Order Requirements at Task Order Award in May 2020

	Contract Type	ATF	DEA	USTP	ATR/GSS	ATR/MSS	JMD/OCIO	OIG ⁴
CLIN 0001 - Transition Services	FFP	X	X	X	X	X	X	X
CLIN 0002 - Program Management	T&M	X	X	X	X	X	X	X
CLIN 0003 - Managed Service Desk Services	FUR and T&M	X	X	X	X		X	X
CLIN 0004 - Account Management and Directory Services	FFP	X	X		X		X	
CLIN 0005 - Unified Communication Services	FFP				X			
CLIN 0006 - Application Hosting Services	FFP		O		O	O	X	X
CLIN 0007 - User (Device) Experience Services (Managed Seat Services)	FUR	X			O		X	
CLIN 0008 - Special Operations	T&M	X			X			
CLIN 0009 - Monitoring and Management Services	FFP	X	X		X		X	
CLIN 0010 - Installation, Move, Add, Change, and Disposal Services	T&M	X	O		O			
CLIN 0011 - Managed Print Service	FUR	X			O			
CLIN 0012 - Innovation/Evolution/DevOps/Software Development/eDiscovery/Special Projects	T&M	X	O		O	X	O	
CLIN 0013 - Travel/Other Direct Costs	CR	X	X	O	O	O	O	O
CLIN 0014 - Contract Access Fee		X	X	X	X	X	X	X

x – Expected and defined at the start of the task order.

o – Expected future use to be defined at a later date.

Source: ATF's Appendix 1 – ESA V Customer requirements.

Office of the Inspector General Audit Approach

Our audit objectives were to assess: (1) ATF's acquisition planning and selection of Leidos for the ESA V task order awarded; (2) ATF's administration and oversight of the task order; and (3) Leidos' performance on the task order, including financial management, monitoring, reporting, and progress toward meeting the task order goals and objectives. The audit scope covered pre-award activities such as ATF's acquisition planning and contract solicitation, ATF's post-award contract administration activities such as oversight of contract performance and review of invoices, and Leidos' performance under the task order in accordance with the PWS and quality assurance surveillance plan.

We interviewed ATF officials at ATF's Headquarters in Washington, DC and by teleconference, including the contracting officer and CORs, as well as program owners at ATF and other federal components. We conducted interviews of JMD Office of the Chief Information Officer's (OCIO) Contract Management Services division and the JMD's PSS. Additionally, we interviewed Leidos personnel at its office in Washington, DC.

⁴ The OIG was excluded from the scope of this audit to comply with federal auditing and independence standards. Appendix 1 includes a detailed explanation of this audit's objectives, scope, and methodology.

We reviewed a sample of monthly progress reports and contractor invoices, and reconciled the invoices to contractor and subcontractor timesheets, approved indirect rates, and supporting documents for other direct costs. Additional information on our audit objectives, scope, and methodology can be found in Appendix 1.

Audit Results

The purpose of ATF's ESA V task order was to maximize the usage of contractor-provided and managed services for IT-related user services in support of ATF, other DOJ components, and other subscribing federal agencies. We found ATF adequately justified its selection of Leidos and performed the appropriate administration and oversight of the task order. However, we found instances where the task order could have been structured differently to ensure it met the federal components' needs, minimized contentions over the scope of work covered by the order, and included performance measures adequate to hold Leidos accountable to the federal components' standards. We also found that Leidos submitted inaccurate monthly reports and ATF did not update its procedures on tracking the completion of required security patches. ATF issued Leidos three Letters of Concern due to scope disagreements and federal components' belief that Leidos was not meeting contract requirements. Lastly, we determined that the Leidos' pricing proposal did not disclose that its price was dependent on federal component participation in the program. As a result, ATF was unaware that a reduction in task order participation by some federal components could lead to rising costs for those that remained.

ATF's Acquisition Planning and Ongoing Contract Management was Appropriate

ATF's contracting team began preparing for the ESA V task order a year prior to the expiration of ESA IV. The contracting officer performed market research and issued a Request for Information to the GSA Alliant 2 contractor pool, from which 17 contractors responded. The contracting officer incorporated various contract types, established performance criteria, and required a Quality Assurance Surveillance Plan (QASP) to monitor the contractor's performance on this performance-based contract. Participating federal components were involved in reviewing the Performance Work Statement (PWS), crafted component-specific requirements to be incorporated into the task order, and reviewed the contractor's proposal on the Technical Evaluation Board. Our assessment concluded that ATF adequately justified its ESA V task order award to Leidos.

We found ATF performed the appropriate administration and oversight of the task order, and some federal components participating in the ESA V program spoke highly of the responsiveness of ATF's contracting team. Additionally, we noted ATF put in place a multi-level invoice review, involving CORs and program owners, which proved effective in identifying billing errors.

Furthermore, we found that Leidos provided weekly status meetings and monthly status reports and responded promptly to ATF's Letters of Concern. We determined that, Leidos accurately billed the federal components on a monthly basis and provided detailed invoices that contained a breakdown of services rendered with the corresponding support based on sampled invoices. Leidos also held meetings to provide updates to the other federal component program owners and leadership.

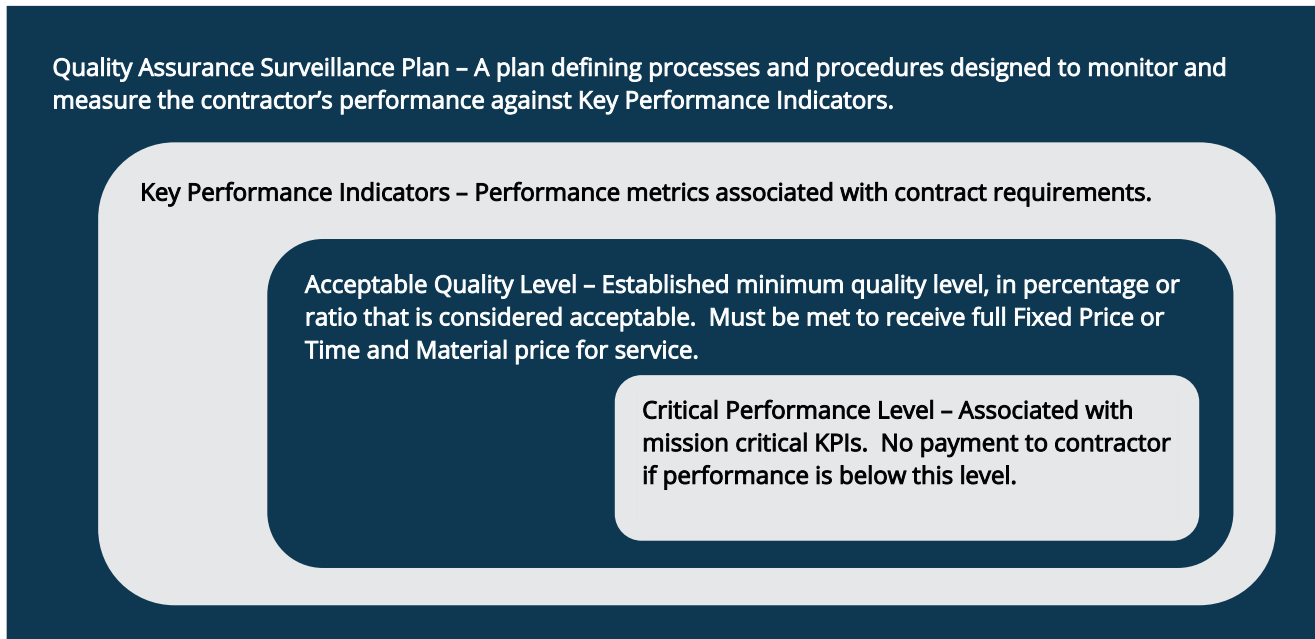
ATF Should Utilize More Effective Key Performance Indicators

The Federal Acquisition Regulation (FAR) Subpart 37.6 states that for performance-based acquisitions, the agencies shall, to the maximum extent practicable, enable assessment of work performance against measurable performance standards to ensure contractor's performance level is meeting contract requirements. To assist with this, ATF's Acquisition Manual dated July 2019 states that, the contracting officer would assist program officials in their tasks of developing performance standards that focus on

mission-oriented results. To monitor contractor's performance, ATF developed key performance indicators (KPI) for tasks, along with the acceptable quality level (AQL) and critical performance level (CPL), if appropriate. ATF also required the contractor to develop a QASP in accordance with the KPIs.

Chart 1

Performance Measurement and Monitoring Tools





Source: OIG analysis of task order acquisition plan, the PWS, and the QASP documents.

Leidos created the required QASP, which was accepted by ATF, identifying 51 KPIs that would be monitored to meet ATF's performance requirements. However, we found that certain KPIs and associated AQLs were inadequate to allow ATF and the federal components to hold Leidos accountable for poor performance. Specifically, we noted that of the 51 KPIs, 5 did not have AQLs established (10 percent) and 20 did not have disincentives (39 percent) for Leidos failing to meet the established AQLs. Additionally, we found disagreements on performance and inadequate KPIs contributed to the problems. For example, ATF program owners and other federal components expressed concerns about instances in which Leidos' monthly status reports indicated AQLs were met, but the Government did not agree with Leidos' assessment. Specifically, ATF officials informed us Leidos was sometimes untimely in meeting contractual tasks, such as replenishing printer cartridges for network printers and installing required IT security patches to mitigate cyber risks, but disincentives were not applied to Leidos' billings in these circumstances. As a result, when Leidos' performance did not meet the expectations of the federal components, disincentives were either not available or not applied to the satisfaction of the participating components. Table 2 includes two examples of KPIs that could have been better defined to adequately hold Leidos accountable.

Table 2

Examples of Key Performance Indicators

	KPI	What We Found	Why it Matters
 Security Patch Installation	<p>The QASP contained two KPIs with an AQL at 100% to ensure Leidos installed 100% of specific types of security patches:</p> <p>1) patch installation mandates from the Department Office of the Chief Information Officer (OCIO);</p> <p>2) critical vendor patches within 30 days of being issued.</p>	<p>We found that disincentives were not assigned to these KPIs to hold Leidos accountable for not meeting the established targets.</p> <p>As discussed in more detail below, we found Department OCIO mandated patches were significantly delayed due to a scope disagreement.</p>	<p>Without impactful disincentives, the government is unable to withhold funds from Leidos for failing to meet requirements.</p> <p>This is a critical component of the PWS/QASP process. Deductions in payment to the contractor could speed up the process in resolving conflicts.</p>
 Multi-Function Printers	<p>The QASP contained a KPI to measure availability for consecutive workdays of multi-function printers provided by a Leidos subcontractor to print, copy, scan, and fax.</p>	<p>One ATF official interpreted this KPI as requiring that all functions be available at all times. However, Leidos defines a printer unavailable when all functions are not operating for two consecutive workdays.</p>	<p>Due to lack of agreement on the KPI, we learned that this KPI is ineffective, as it is rare for a multi-function printer to be entirely unavailable, even though there might be times when some critical functions are unavailable.</p>

Source: OIG analysis of the QASP and the KPIs.

We shared the results of our review of KPIs and discussed details of several KPIs with ATF. ATF’s contracting officer informed us that ATF did discuss KPIs with participating federal components during the acquisition phase of the task order award. However, the contracting officer acknowledged the KPIs have not been reevaluated since the award to ensure Leidos is meeting the needs of the participants and contract requirements. ATF also stated that sometimes a financial disincentive may not always be required for all KPIs, suggesting that when KPIs are not met, the parties should collaborate to determine what is required to improve performance. We believe financial disincentives should be applied to critical KPIs such as security patching to influence contractor efforts to achieve expected performance levels. When discussing the KPI for installing security patches, ATF was unable to explain how it set the targets or why disincentives were not included. ATF’s contracting officer explained that the same outside consultant who assisted ATF in the acquisition process also developed the KPIs, that this consultant was no longer under contract with ATF. We found that ATF did not retain adequate records on how the KPIs were developed with the consultant. For a contract with a 9-year period of performance, ATF should have maintained documentation related to how

required performance metrics were developed by the outside consultant and should also have an internal knowledge base on performance metrics and needs, separate from the outside consultant.⁵

A robust QASP with well-defined KPIs and meaningful disincentives is a critical oversight tool for ensuring Leidos' adequate performance of contract responsibilities. Therefore, we recommend that ATF involve all participating federal components in a review of KPIs, revise those KPIs that need clarification, include disincentives where appropriate, retain supporting documentation on the development of the performance measures, and work with Leidos to modify the contract. We also recommend that ATF implement procedures to conduct periodic assessments to determine how current KPIs could be modified and whether new KPIs should be added to adequately address the government's need.

ATF Should Better Engage Participating Federal Components

During our discussions with JMD, the task manager expressed concerns about ESA V's shifting CLIN contract types away from a T&M to a FFP model. Under the previous ESA IV task order, each federal component had specific CLINs to meet its requirements, instead of the more service-specific CLINs of ESA V. For example, under ESA IV most subscribing components had a component-specific T&M CLIN with additional other cost-type CLINs, as needed. However, under ESA V, ATF no longer offered federal component-specific CLINs, and many of the services that had been included in T&M CLINs under the previous task order shifted to a FFP model. ATF's contracting officer explained that this decision was made during the award process to realign several contracted services, such as the application hosting and account management services, to a FFP model to obtain contract efficiencies. However, we believe that this shift away from a T&M model reduced flexibility within the task order and contributed to scope contentions between Leidos and the federal components.

JMD Expressed Concerns About Contract Cost Model Prior to Award

In February 2020, prior to the ESA V task order award, ATF reached out to the participating federal components for their validation that the PWS requirements fit their needs and for input on the contractor's proposed pricing. In response, JMD expressed concerns to ATF's contracting officer that the majority of their needed services fell under FFP CLINs, and there were no suitable T&M CLINs to which JMD could subscribe. JMD additionally expressed concerns regarding Leidos' FFP price proposal, as it appeared to be too low compared to historical costs. JMD further stated that if Leidos' assumptions on increasing performance efficiency allowing for decreasing cost methodology did not come to fruition, JMD may be faced with higher overall costs for which funds had not been budgeted.⁶ However, JMD informed us that ATF's contracting officer never provided a response to its pricing concerns prior to the contract award.⁷

⁵ The FAR Subpart 4.801 requires that contract file documentation be sufficient to constitute a complete history, such as background information related to the acquisition process.

⁶ The FAR 16.1 discusses selection of contract types and states that contract type and prices are closely related and should be considered together. With the objective being to negotiate a contract type and price that will result in reasonable contract risk and provide the greatest incentive for efficient and economical performance.

⁷ According to ATF's contracting officer, the federal components were engaged before the bid solicitation was issued and advised of the CLIN structure and contract type. Also, federal components had representatives on the technical evaluation team during the original award.

JMD informed us that, after the task order was awarded, Leidos planned to replace its network operations contract personnel, who were working under an FFP CLIN, with lesser qualified workers to cut costs. JMD felt these new workers would lack the skill, experience, and institutional knowledge to meet JMD's requirements. Unlike T&M CLINs, which contain specific worker qualifications, JMD was unable to prescribe how Leidos staffed the work performed under the FFP CLINs.⁸ Therefore, JMD could not prevent Leidos from replacing the experienced network engineers with other contractor personnel whom Leidos believed could perform the work. JMD had previously experienced performance issues with the Leidos staff working on this project, which resulted in JMD drafting a Letter of Concern. JMD informed us that it feared Leidos replacing the current workers with cheaper and potentially less-effective workers risked the network services provided to JMD and the DOJ as a whole. To prevent this, JMD renegotiated and modified its order with Leidos to allow the current Leidos staff to remain in place by increasing Leidos' contract award amount in September 2022. As a result, JMD added \$19.1 million over the next 2 years under FFP, FUR and T&M CLINs to retain current Leidos staff as well as to provide after-hours critical network support on a T&M basis, supporting ongoing special operations, and hire 8 new key positions.

Performance Work Statements Should be Better Aligned and Documented to Avoid Scope Disagreements

Since the task order award in May 2020, ATF's contracting officer has received concerning feedback from the federal components regarding Leidos' performance, resulting in a total of six Letters of Concern being drafted or issued to Leidos. We found the ESA V's shift to more of a fixed price model reduced the government's ability to modify work orders from Leidos. This has created several scope contentions and delayed necessary projects.

ATF's Acquisition Manual Subpart 37.6 states that the program office, with the contracting officer's assistance, should develop an accurate and complete PWS that defines the desired outcomes. In ESA V, the PWS defined general requirements for all federal components, and component specific requirements were defined in an appendix to the PWS. In several instances, we determined that the government and Leidos had different interpretations of the PWS requirements. This resulted in Leidos contending that several of the government's work requests fell outside the PWS and thus was not priced as part of Leidos' original fixed price proposal. In these instances, Leidos would propose the government modify the contract to add the requested work under a T&M CLIN, at additional cost to the government.

In November 2021, Leidos began to track ESA V scope contentions in a scope determination log. In the first 6-month period ending April 2022, Leidos had logged 10 federal component work requests it believed require further review. Subsequently, per our inquiry of any scope contentions prior to November 2021, Leidos added three additional work requests to the log. Of the 13 work requests, 11 were related to FFP CLINs, 1 was related to a T&M CLIN, and 1 needed additional clarification from the requestor. We reviewed this log and found that of the 12 work requests not needing additional clarification, 7 requests were later determined by Leidos to be within scope, and five requests out of scope. Our analysis shows it took an average of 11 days for Leidos to decide whether work requests were within or out of scope and before work

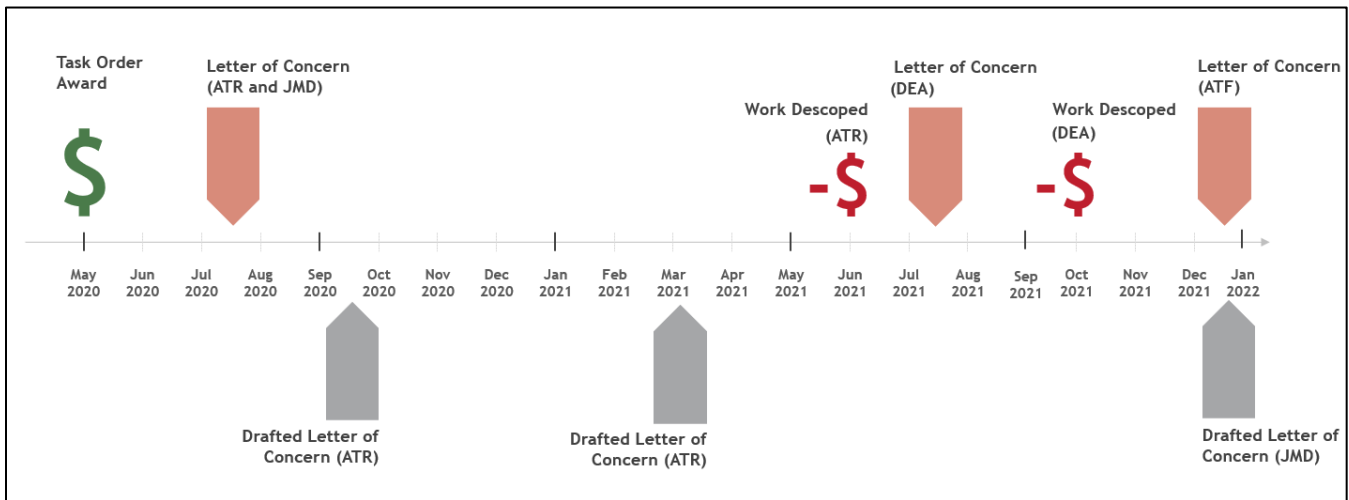
⁸ Under a FFP contract type, a contractor is responsible for meeting performance standards and can unilaterally determine the number of labor hours or skill mix. Thus, a FFP contract type is not suitable for complex projects and does not lend itself to modifications and flexibility. Customers cannot adjust the scope of the project without negotiating new terms and possibly delaying work. In contrast, a T&M contract type provides customers a more dynamic and transparent solution, allowing for more flexibility.

began on a task.

In total, the contracting officer has issued three Letters of Concern and drafted three additional Letters of Concern that were resolved prior to being formally issued. Chart 2 shows the timeline of issued and drafted Letters of Concern since the task order award in May 2020.

Chart 2

Timeline of Letters of Concern



Source: OIG analysis of task order award and Letters of Concern.

Performance issues discussed in the six Letters of Concern, whether issued or not, were addressed and resolved. Table 3 provides a summary of the issues described within the Letters of Concern and the resolutions.

Table 3

Letters of Concern Issued by ATF

Date	Federal Component	Summary of Issues	Resolution
July 17, 2020 (Issued)	ATR and JMD	<p>ATR: Leidos determined projects previously performed under ESA IV was outside the scope of the newly awarded ESA V and requested to be added to the task order as special projects.</p> <p>JMD: Scope contention over five projects related to the application hosting that Leidos requested to be added to the task order as special projects.</p>	ATF directed Leidos to perform disputed projects with no increase in contract price or risk being in breach of contract. A formal resolution/closure of the Letter of Concern was not necessary.
September 2020 (Draft) & March 2021 (Draft)	ATR	<p>September 2020: Leidos did not complete a project in a timely manner due to resource shortage and refused to provide additional resources without additional funding.</p> <p>March 2021: Leidos was unable to provide accurate report of specific assets. ATR also experienced issues related to security patches, customer support, video conferencing application, and new hire account creation.</p>	According to ATR, the September 2020 Letter of Concern was resolved after ATF intervened and facilitated meetings with Leidos and ATR, after which Leidos improved its performance. However, ATR later experienced the same performance issues and had to draft another letter of concerns in March 2021. Ultimately, ATR decided to descope from the task order in lieu of issuing the letter.
July 15, 2021 (Issued)	DEA	Not meeting performance standard on seven separate work areas covering communication, timeliness of help tickets resolution, travel requests, user account creation, and customer complaints regarding customer service and software latency issues.	This Letter of Concern was officially resolved with no increase in contract price and closed on September 13, 2021. DEA descope from the task order in October 2021.

Date	Federal Component	Summary of Issues	Resolution
December 20, 2021 (Issued)	ATF	Scope contention regarding security patches, communication, and not properly cleaned up aging accounts. This letter is discussed in detail later in our report.	This Letter of Concern was officially resolved with no increase in contract price and closed on February 8, 2022.
December 2021 (Draft)	JMD	Leidos onboarded two unqualified network security engineers and put JMD's network at risk. JMD also experienced issues related to communication and Leidos' network monitoring and emergency incident responses.	JMD's task manager informed us that the process of completing this Letter of Concern was delayed and JMD was able to work with Leidos to resolve the performance issues, prior to being issued.

Source: OIG analysis of the Letters of Concern.

We believe ATF did not ensure federal components had a clear understanding of the contract types and their restrictions prior to awarding the task order. The ESA V fixed-price cost structure is not suitable for all federal components' requirements and has contributed to the escalating costs under this task order. ATF's procurement office should have discussed and addressed JMD's concerns regarding the contract types to ensure the CLINs would meet its needs. In addition, the switch to a fixed price model and differing interpretations between federal components and Leidos on the scope of work within the PWS have contributed to scope disagreements and delays in service. As a result, more than half of work requests questioned by Leidos were determined to be in-scope, and therefore were unnecessarily delayed and left risks unmitigated until scope contentions were resolved. We recommend ATF develop procedures for future acquisitions that fully engage federal components in ensuring their concerns are adequately addressed prior to contract award and that includes controls to review and ensure the contract structure meets participating components' mission requirements. Additionally, we recommend that ATF work with the participating components on evaluating options in modifying the option years of the ESA V task order to ensure the available CLINs and PWS interpretations are aligned and fully documented to minimize scope contentions and risk to component missions and objectives.

Leidos Should Meet Security Patch Deadlines and Submit Accurate Monthly Reporting

Of the Letters of Concern previously discussed, one of the most troubling was the December 20, 2021 letter addressing Leidos' failure to complete ATF's IT system security patches within required deadlines. During our audit we examined the circumstances of this incident and found it to be an example of how scope contentions between the Government and Leidos could lead to the Department's IT systems being left vulnerable.

On November 3, 2021, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), issued a directive that identified 102 vulnerabilities that were required to be remediated by Federal agencies before due dates, ranging from November 17, 2021, through

December 1, 2021.⁹ We found that ATF missed these deadlines and Leidos' monthly reporting failed to accurately identify the missed deadlines.

Meeting Deadlines on Security Patch Installations

On November 5, 2021, ATF provided Leidos the CISA directive and listing of patches required for immediate remediation. Although the directive was new, the security vulnerabilities identified had been previously submitted and included in Leidos' responsibilities. ATF's notification to Leidos left them 12 days to meet the earliest patch deadline. Unfortunately, although Leidos stated the application of patches were in-scope, their position was that in order to meet the more stringent timelines documented in the directive, additional staff would be needed, at an additional cost to the Government. While discussions continued through email exchanges between Leidos and ATF for another 14 days, Leidos stated that it did not stop performing security patches during the ongoing discussions with ATF; however, it could not provide data to support that work. Ultimately, the contracting officer made the final decision on November 19 that the installation of the patches was within the scope of Leidos' responsibilities and directed Leidos to perform the work at no additional cost. On that same day, the Department OCIO issued an alert based on the CISA directive that 94 vulnerabilities be remediated by December 1, 2021.¹⁰ According to the November 30, 2021, Security Posture Dashboard Report (SPDR) from the Department OCIO, 35 unaddressed cyber vulnerabilities (37 percent) affected 980 devices, such as servers, workstations, and conference room systems.¹¹ The contracting officer issued a Letter of Concern on December 20, 2021, 45 days after the original request and 33 days after the earliest CISA deadline, documenting Leidos' unwillingness to perform the in-scope work. Nevertheless, the critical deadline had passed, and some ATF IT equipment had been left at risk due to security patches not yet installed. Leidos complied and worked on fulfilling the Department OCIO alert, and by January 11, 2022, the number of devices not fully updated with the necessary security patches had reduced to 118 devices. On February 8, 2022, ATF officially closed the Letter of Concern, agreeing with Leidos' corrective actions. As this example demonstrates, scope contentions can lead to missed deadlines, which in this case resulted in unmitigated risks to known security vulnerabilities.

Monthly Reports that Discuss Progress and Challenges

We determined that while dealing with ongoing scope contentions, Leidos did not accurately self-assess its performance on the monthly status reports provided to the federal components. We observed in Leidos' November 30, 2021 monthly status report to ATF dated December 21, 2021, that Leidos did not mention the

⁹ Created in November 2018 (Pub. L. No. 115-278), the CISA coordinates with federal entities in carrying out cybersecurity and critical infrastructure security activities. The CISA manages a catalog of cyber vulnerabilities and issued its Binding Operational Directive No. 22-01 on November 3, 2021, a compulsory direction to federal, executive branch departments, and agencies on safeguarding federal information systems, in part, by remediating vulnerabilities from that catalog.

¹⁰ The Justice Security Operations Center (JSOC), a part of the Department OCIO, evaluates software patches and issues alerts called Vulnerability Patch Requirements (VPR) when a vulnerability is determined to be a high risk to the Department. After reviewing the CISA directive and the 102 vulnerabilities, the JSOC issued a VPR on November 19, 2021, which eliminated 15 that had been addressed in prior VPRs and added 7 that were perceived to be a risk to the Department.

¹¹ The SPDR from the Department's OCIO provides DOJ components daily status of vulnerabilities found on IT assets and trends over time.

Department OCIO's alert issued on November 19 or the frequent and urgent discussions it had with ATF in November 2021, which we obtained from ATF, on the challenges of complying with government mandates on security patching. Leidos explained that because the OCIO's alert was not due until December 1, it did not need to mention the challenges of meeting the patching deadline in the November report.

In another example, Leidos' monthly reports from August 2020 and September 2020 reported that it was 100 percent timely on ATR's system security patching and provided no written comments. However, ATR stated that Leidos did not meet an August 21, 2020 security patch deadline set by the Department OCIO and that 84 assets had remained unpatched as of August 27, 2020. ATR officials expressed their frustration with the disparity between Leidos' reporting of 100 percent compliance in the monthly reports and unaddressed vulnerabilities of ATR IT assets. Leidos had responded to ATR that the shortfall was due to ATR end users not connecting their devices to the network at a minimum of once a month to allow the updates to occur. During our audit, Leidos also informed us that it calculated the 100 percent compliance based on servers that had been patched, as specified in the QASP, which excludes workstations in meeting timeframes of system security patch installation required by the Department OCIO. We believed that Leidos could have included in these monthly reports its calculation methods and the challenges of security patch installation due to end users' behavior to address ATR's concerns.

According to the PWS, Leidos was to provide federal components with monthly status reports that contain their compliance levels, and also briefly summarize management and technical progress and challenges. Although the contracting officer and program officials met monthly to verify the accuracy of Leidos' monthly status reports, we believe Leidos' monthly status reports provided to ATF and ATR were inaccurate and did not identify challenges and contentions it was working through at that time. Thus, we recommend that ATF work with Leidos to ensure its monthly status reports accurately summarize its performance, technical progress, and challenges, as required. We additionally recommend that ATF implement procedures to ensure federal components review and identify inaccuracies and incompleteness in Leidos' monthly status reports.

ATF Should Update its Procedures for Documenting Security Patching

During our testing of Leidos' completion of required security patching under the CISA directive, we observed that ATF did not update its standard operating procedures (SOP) when they moved to a new tracking method. ATF's April 2021 SOP stated that reports from agency's IT scanning tools be used to track individual cyber vulnerabilities from inception to completion and required staff to track the testing of security patches by creating an internal record in ATF's IT support portal. When we requested this documentation related to the November 2021 Department OCIO alert, which identified 94 cyber vulnerabilities be remediated by December 1, 2021, ATF provided reports not mentioned in the April 2021 SOP, which could not account for security patching from start to finish, a change that an ATF official acknowledged was not updated in the SOP. Instead, to support our request for documentation on the Department OCIO alert, ATF provided us with a SPDR queried on November 30, 2021, a day before the final deadline of the CISA directive. The report showed that 35 cyber vulnerabilities (37 percent) were still being addressed, affecting 980 devices, as previously discussed. However, as the SPDR is only a snapshot of unremediated vulnerabilities at a specific point in time, neither Leidos nor ATF could provide us with documentation demonstrating the timely remediation of the vulnerabilities from the CISA directive that were no longer listed on the SPDR.¹²

¹² In October 2021, about 1 month before the CISA directive was issued, the Department OCIO released a new version

According to ATF, as of October 2022, only two of the 94 vulnerabilities from the November 2021 Department OCIO alert remained unresolved. Finally, the last two vulnerabilities were resolved in March 2023.

Devices that have not been secured with required patches increase the risk of cyber incidents. Combined with a lack of reports demonstrating the detailed records of how cyber vulnerabilities were tested, remedies deployed, and fully remediated, ATF may find it difficult to hold Leidos accountable in identifying and troubleshooting cyber incidents if they were to occur. Consequently, we recommend ATF update their SOPs for security patch implementation to ensure reports and records are retained that track remediation efforts from start to finish.

ATF Should Perform Forecasting and Risk Assessments to Determine Impact of Changing Participation

For the ESA V task order, Leidos proposed a decreasing FFP price model based on its belief that, as more federal components subscribe to the ESA V task order, Leidos' staff could serve multiple federal components more efficiently, thereby achieving cost savings over time. Based on that assumption, Leidos' option years were priced significantly lower than the base years.¹³ However, as previously discussed in this report, ATR and DEA descope from the ESA V program. Unable to realize the efficiencies of scale it originally intended, Leidos submitted to ATF's contracting officer a modified cost proposal in September 2021, increasing its costs for base year 2 through option year 6 of the contract.¹⁴ The contracting officer stated that Leidos' original bid proposal did not explain the possible cost impact (i.e., increased cost) to the remaining participants should federal components decide to descope or leave the program. In addition, the proposal did not contain language indicating that the FFP elements are tied to other federal components' participation. Per FAR 39.102, an agency should analyze risks, benefits, and costs. Reasonable risk taking is appropriate as long as risks are controlled and mitigated. Contracting and program officials are jointly responsible for assessing, monitoring, and controlling risk when selecting projects for investment and during program implementation.¹⁵ We found that the ESA V task order's shared cost model and the cost variability was not fully disclosed by Leidos or understood by ATF and other federal components, and ATF did not consider the risk of federal components descope or withdrawing from the program.

We believe that the ineffective performance measures and lack of clarity of the PWS that we previously discussed contributed to ATR's reduction of work with Leidos. In June 2021, ATR reduced 26 percent of its scope of work from the ESA V program because it reportedly faced many challenges and was not satisfied with Leidos' performance. The DEA was also experiencing performance issues with Leidos. In

of the SPDR to all components that could retain historical data for tracking, review, and analysis of vulnerability patching status.

¹³ The ESA V task order includes one 10-month base period, two 12-month base years, and six 12-month option periods.

¹⁴ Leidos' modified cost proposal requested an additional \$2.1 million from ATF and \$6.1 million from JMD.

¹⁵ FAR 39.102 states that appropriate techniques should be applied to manage and mitigate risks during the acquisition of IT, including but not limited to thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures.

October 2021, DEA descoped the majority of their ESA V work. According to the DEA, ATF was aware of DEA's intention to consolidate its IT contracts into one large contract and that its participation in the ESA V task order was only temporary; the DEA awarded its own large IT contract in July 2021.¹⁶ As previously stated, Leidos responded to the ATR and DEA descoping by submitting a modified cost proposal and additionally noted that there would be further cost impacts to the remaining participants if additional federal components descoped their work from the ESA V program. However, since the cost impact proposal was under ATF's review for an extended period of time, Leidos informed us in August 2022 that the proposal was no longer valid and withdrew it. As of June 2023, Leidos has not submitted any updated cost adjustments associated with federal components leaving the ESA V program.

Despite federal components descoping services or leaving the program, the overall ESA V task order value has increased 85 percent since being awarded in May 2020, from the initial task order value of \$396.9 million to over \$733.3 million as of the end of November 2022, as shown in Table 4.¹⁷ As of the end of November 2022, 90 modifications had been issued against the task order. New component joined and original participants expanded their use of ESA V services. For instance, the Criminal Division joined shortly after the award, and in January 2021, DEA expanded its scope to include Radio Communications Support. There have also been key reductions in scope from the program, such as ATR descoping part of its work in June 2021 and DEA descoping most of its work in October 2021, keeping only the Radio Communication Support services. Additionally, ATF's task order costs have increased \$340 million (286 percent), and JMD's have increased \$74 million (88 percent).¹⁸

¹⁶ DEA stated it was unable to provide the email correspondence notifying ATF before the task order was awarded that DEA participation in ESA V was only temporary. In contrast, ATF informed us that DEA notified ATF of its plan to descop from the ESA V task order on July 27, 2021, which was after the award of the task order.

¹⁷ Since November 2022, the Federal Bureau of Prisons joined the ESA V task order and the remaining federal components added additional work.

¹⁸ The contractor who previously provided ATF cloud hosting support was acquired by Leidos in January 2020, and had become as a wholly owned subsidiary of Leidos.

Table 4

ESA V Federal Components and Estimated Order Values

Federal Components	ATF	DEA	USTP	ATR	JMD-OCIO	OIG	CRM	Total Value
Original Estimated Value (May 2020)	\$118,831,919	\$120,083,009	\$3,041,027	\$65,166,790	\$84,856,898	\$4,963,915	\$0	\$396,943,558 ¹⁹
Current Estimated Value (November 2022)	\$459,272,407	\$18,145,197	\$3,041,027	\$53,800,473	\$159,643,016	\$860,170	\$38,563,304	\$733,325,594
Increase In Percentage	286%	-85%	0%	-17%	88%	-83%	N/A	85%

Source: ATF's ESA V pricing summary as of November 2022.

During the task order proposal and award period, the Department did not understand the cost impact of any reduction in scope or participation to remaining ESA V participants. However, now ATF is aware that Leidos may request additional costs due to federal components' departure from the program. The increased costs may negatively impact agencies' budgets, as agencies would have to allocate additional money for ESA V services for which they had not planned. We believe that ATF should ensure all federal components within the ESA V program understand the cost sharing model and determine their future level of commitment to the program. Thus, we recommend that ATF implement procedures to perform forecasting and risk assessments with the program owners during the acquisition planning phase and throughout the task order performance, in compliance with the FAR.

¹⁹ The original estimated value did not include contract access fee of \$1,350,000 and a portion of the CLIN 12 special project of \$94,429,559. For special project, ATF awarded the base contract at not to exceed amount of \$160,000,000 instead of the estimated value of \$65,570,441.

Conclusion and Recommendations

Our audit of ATF's award and management of the ESA V task order identified areas for improvement. While federal components spoke highly of the responsiveness of ATF's contracting team, we determined that the PWS left room for interpretation and ESA V's shifting contract types away from a T&M to a FFP model led to scope contentions between the federal components and Leidos. These disagreements led to unnecessary delays and allowed vulnerabilities to persist long beyond government-wide deadlines. At the same time, these challenges were not accurately reported in Leidos' self-assessed monthly status reports. ATF also did not update its own procedures of retaining definitive records on installation of the required security patches, which exposed its missions and operations to cyber risks. We also found that ESA V performance standards as defined by the KPIs and AQLs may not have adequately addressed the federal components' requirements or did not have disincentives to assist the Government in ensuring Leidos met the performance expectations. ATF also did not fully understand Leidos' pricing assumptions. Thus, when certain federal components descope their orders, Leidos proposed a redistribution of cost by increasing the cost borne by the remaining federal components. In addition, ATF did not adequately address federal components' concerns regarding the suitability of contract types available in ESA V, leading a federal component to modify its orders and allocating additional funds not previously budgeted.

We recommend that ATF:

1. Involve all participating federal components in a review of its KPIs, revise those KPIs that need clarification, include disincentives where appropriate, retain supporting documentation on the development of the performance measures, and work with Leidos to modify the contract.
2. Implement procedures to conduct periodic assessments to determine how current KPIs could be modified and whether new KPIs should be added to adequately address the government's need.
3. Develop procedures for future acquisitions that fully engage federal components in ensuring their concerns are adequately addressed prior to contract award and that includes controls to review and ensure the contract structure meets participating components' mission requirements.
4. Work with the participating components on evaluating options in modifying the option years of the ESA V task order to ensure the available CLINs and PWS interpretations are aligned and fully documented to minimize scope contentions and risk to component missions and objectives.
5. Work with Leidos to ensure its monthly status reports accurately summarize its performance, technical progress, and challenges, as required.
6. Implement procedures to ensure federal components review and identify inaccuracies and incompleteness in Leidos' monthly status reports.
7. Update their SOPs for security patch implementation to ensure reports and records are retained that track remediation efforts from start to finish.

8. Implement procedures to perform forecasting and risk assessments with the program owners during the acquisition planning phase and throughout the task order performance, in compliance with the FAR.

APPENDIX 1: Objectives, Scope, and Methodology

Objectives

The objectives of this audit were to assess: (1) ATF's acquisition planning and selection of Leidos, Inc. (Leidos) for the Enterprise Service Architecture V (ESA V) task order awarded; (2) ATF's administration and oversight of the task order; and (3) Leidos' performance on the task order, including financial management, monitoring, reporting, and progress toward meeting the task order goals and objectives.

Scope and Methodology

We reviewed ATF's Enterprise Standard Architecture V (ESA V) task order awarded to Leidos, worth an estimated \$733.3 million with a 9-year period of performance of May 1, 2020, through April 30, 2029. The audit scope covered pre-award activities such as ATF's acquisition planning and contract solicitation, ATF's post-award contract administration activities such as oversight of contract performance and review of invoices, and Leidos' performance under the task order in accordance with the PWS and quality assurance surveillance plan.²⁰ As of September 2022, ATF has paid Leidos \$173.5 million for its services under this task order.

To address our objectives, we interviewed ATF officials at ATF Headquarters in Washington, DC. We reviewed the ESA V task order contract file, analyzed Letters of Concern ATF issued to Leidos, and interviewed the contracting officer, contracting officer representatives, as well as ATF and other federal components' program owners. We also interviewed other DOJ component officials, to include an IT Specialist at the JMD OCIO's Contract Management Services division and the Assistant Director of the Acquisition Management Group at JMD Procurement Services Staff. We also interviewed Leidos personnel at its Program Management Office in Washington, DC. We reviewed a sample of monthly progress reports, contractor invoices and reconciled them to contractor and subcontractor timesheets, approved indirect rates, and supporting documentation for other direct costs. We also reviewed relevant Federal Acquisition Regulation (FAR), ATF procedures, and Cybersecurity and Infrastructure Security Agency directives applicable to the ESA V task order.

Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit 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.

²⁰ Though the Office of the Inspector General (OIG) was a component-level customer under the ESA V task order, the OIG descope its remaining work in November 2021 and no longer participates under the task order. For the purposes of this audit, the OIG remained independent with respect to this task order, and we excluded the OIG costs (0.12 percent of the original task order amount) and associate activities from our audit.

Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objectives. We did not evaluate the internal controls of ATF and Leidos to provide assurance on its internal control structure. ATF and Leidos' management are responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123 and the FAR. Because we do not express an opinion on ATF and Leidos' internal control structure, we offer this statement solely for the information and use of ATF and Leidos.²¹

We assessed the design, implementation, and operating effectiveness of these internal controls and identified deficiencies that we believe could affect ATF and the federal components' ability to effectively and efficiently operate, to correctly state financial and/or performance information, and to ensure compliance with laws and regulations. The internal control deficiencies we found are discussed in the *Audit Results* section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the objectives of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Compliance with Laws and Regulations

In this audit we tested, as appropriate given our audit objectives and scope, select transactions, records, procedures, and practices, to obtain reasonable assurance that ATF and Leidos' management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of our audit. Our audit included examining, on a test basis, ATF and Leidos' compliance with the following laws and regulations that could have a material effect on ATF and Leidos' operations:

- FAR Part 4.8: Government Contract Files
- FAR Part 6: Competition Requirements
- FAR Part 7: Acquisition Planning
- FAR Part 10: Market Research
- FAR Part 15: Contracting By Negotiation
- FAR Part 16.601: Time-and-Material Contracts
- FAR Subpart 1.6: Career Development, Contracting Authority, and Responsibilities
- FAR Subpart 2.101: Definitions
- FAR Subpart 37.6: Performance Based Acquisition
- FAR Subpart 42.15: Contractor Performance Information
- FAR Subpart 46.401: Government Contract Quality Assurance

This testing included analyzing award files and related documentation, interviewing agency contracting officials, other federal component task managers, and Leidos officials, and reviewing invoices and supporting documentation. As noted in the Audit Results section of this report, we found that ATF did not

²¹ This restriction is not intended to limit the distribution of this report, which is a matter of public record.

comply with federal regulations related to contract file documentation and establishing performance standards to enable assessment of contractor work performance. We also determined that ATF could improve upon its pre-award procedures and risk assessment. Nothing came to our attention that caused us to believe that ATF and Leidos did not comply with federal regulations related to invoicing and whistleblower protections.

Sample-Based Testing

To accomplish our audit objective, we performed sample-based testing for Leidos' monthly status reports and invoices to ATF and other federal components, specifically verifying the accuracy of billed labor rates, labor hours, and other direct costs. In this effort, we employed a judgmental sampling design to obtain broad exposure to numerous facets of the areas we reviewed. This non-statistical sample design did not allow projection of the test results to the universe from which the samples were selected.

Computer-Processed Data

During our audit, we obtained information from Leidos' timekeeping system. We did not test the reliability of those systems as a whole, therefore any findings identified involving information from those systems were verified with documentation from other sources.

APPENDIX 2: ESA V CLIN Descriptions

CLIN	CLIN Descriptions
CLIN 0001 - Transition Services	To conduct an orderly migration of the infrastructure and services from current contractor to their interim state and to the Managed Services Solution as defined under the task order.
CLIN 0002 - Program Management	To provide a consolidated Program Management Office (PMO) that supports all federal components. The PMO shall publish a monthly newsletter, provide highlights of major accomplishments, and develop and deliver a program management plan.
CLIN 0003 - Managed Service Desk Services	To provide a Managed Service Desk (MSD) solution (including all Contractor recommended tools) that supports the federal component. The MSD shall provide all of the functionality of the current Information Technology Services Management in a consolidated, effective, and efficient manner for the federal components.
CLIN 0004 - Account Management and Directory Services	To provide administration and support option to all software including managing/maintaining the Active Directory and its environment, the addition and removal (provisioning) of users, managing the domain controllers, providing monitoring support, and providing tier 1 service desk support.
CLIN 0005 - Unified Communication Services (UCS)	To provide a federal component a-secure UCS that fully integrates real-time communications with non-real-time communications in order to support their Managed Services Solution, to include refresh, Installation, Move, Add, Change and Disposal (IMACD) Services, transmissions usage accounting / management, and monitoring & management services related to a unified approach to end user communications.
CLIN 0006 - Application Hosting Services	To provide a web-based portal with automated alerts based on the thresholds that inform the government of degradation or loss of application and infrastructure services.

CLIN 0007 - User (Device) Experience Services (Managed Seat Services)	<p>To maintain the current desktop/laptop (user-experience) services with the goal of maintaining version currency on both software and hardware. For example, the contractor is responsible for managing, maintaining, issuing, replacing, upgrading, and keeping an inventory of the cellular/wireless devices and the user(s) assigned to the equipment, providing full-service billing management for all cellular/wireless/landline service providers, and developing and supplying an ever-evolving solutions.</p>
CLIN 0008 - Special Operations	<p>To provide a Special Operation Team to support each federal component that functions as a self-sufficient operation that will deliver the rapid deployment of communications and IT services during emergency responses, disaster recovery operations, relocations, or special events. For example, the contractor shall provide direct, on-site, or indirect on-site or remote support for the deployment of IT for critical incidents, National Security Special Events, declared disasters, presidential conventions, etc.</p>
CLIN 0009 - Monitoring and Management Services	<p>To monitor, using a screen mounted in the service desk and/or network operations area, the entire network configuration. If a problem is noticed, the contractor shall notify the Government contact about the difficulty and place a ticket in the IT Service Management system that will be handled and managed by the contractor. Also, the contractor shall ensure that infrastructure performance criteria contained in the Key Performance Indexes are maintained for all operational capabilities.</p>
CLIN 0010 - Installation, Move, Add, Change, and Disposal (IMACD) Services	<p>To provide IMACD services for any existing or new device or software of the federal component environments based on the Standard Operating Procedures of the General Support System documentation and the standards of Key Performance Indexes. IMACDs apply to both physical and logical items and are differentiated by those requiring a site visit and those that can be fixed remotely. The Contractor shall perform IMACDs at all federal component sites (CONUS and OCONUS).</p>
CLIN 0011 - Managed Print Services (MPS)	<p>To provide MPS for the provisioning of each federal component site's requirements for all devices and software (print, copy, scan, fax) in support of the Managed Services Solution.</p>

<p>CLIN 0012 - Special Projects</p>	<p>Based on Government-approved results of the Contractor-provided Technology White Papers and briefings the contractor shall provide a detailed project plan, pilot, test, and document the proposed upgrade, and implement the upgrade based on government approval of the pilot result.</p>
<p>CLIN 0013 – Other Direct Costs (ODCs)</p>	<p>To purchase hardware, software, and related supplies critical and related to the services being acquired under the task order. ODCs must be authorized and approved prior to any purchase by the contracting officer representative and will be reimbursed for actual costs as provided in the contract.</p>
<p>CLIN 0014 – Contract Access Fee (CAF)</p>	<p>The task order includes a CAF of \$150,000 in a 12-month performance period. CAF reimburses General Services Administration for the cost of developing and operating its Government-wide Acquisition Contract Alliant 2 contract.</p>

APPENDIX 3: Federal Components' Task Order Descriptions

Federal Components	Task Order Descriptions
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)	ATF enforces Federal laws and regulations relating to alcohol, tobacco, firearms, explosives, and arson. ATF required a contractor to provide service desk support to approximately 7,540 active directory users and limited external users, direct access to technical support service by a limited number of headquarter staff, daily reporting on the status of calls, for executive level support, account management and directory services, user experience services, special operations (office moves and law enforcement operations, exercises, training operations and deployments) services, continuity of operations/disaster recovery, security monitoring and management services, IMACD services, managed print services at 250 locations with 7,000 users using approximately 875 devices, and special projects.
Drug Enforcement Administration's (DEA) Merlin	The DEA is responsible for enforcing the controlled substances laws. DEA Merlin (DEA's classified infrastructure) required a contractor to provide technical support in the categories of System/Network Administration, Service Desk support, Operating System level Database Administration, Systems Engineering Maintenance, and Information Assurance on all domains, both classified and unclassified. Provide Merlin Information Resource Specialists to perform maintenance visits required to sustain operations.
Drug Enforcement Administration's (DEA) Narcotics Enforcement Data Retrieval Systems (NEDRS)	DEA required a contractor to provide computer system expertise to assist DEA personnel with system engineering, software development and operational support for DEA intelligence and analytical applications. The contractor shall provide the personnel necessary to continue to develop, implement, integrate, maintain, and enhance version of the NEDRS. The contractor is required to use an agile software development approach in building software for DEA. Provide project management, user support, various system and application maintenance support. Assist with IT security and support for the National License Plate Reader Network and application.

<p>United States Trustee Program (USTP)</p>	<p>The USTP is the component of the Department of Justice responsible for overseeing the administration of bankruptcy cases and private trustees. The USTP requires efficient and dependable service desk support for the UST program users. UST's service desk supports all IT-related requests by the entire UST program community.</p>
<p>Antitrust Division's (ATR) General Support System (GSS)</p>	<p>The ATR is responsible for enforcing and providing guidance on antitrust laws and principles. The ATR GSS is managed by the Office Automation Staff and consists of the unclassified infrastructure and IT services for the division. The GSS is responsible for end user support to include asset management and training, program and project management, engineering and operational engineering, systems operations and administration to include telecommunications, and operational IT security.</p>
<p>Antitrust Division's Management System Staff (MSS)</p>	<p>The MSS office is responsible for developing and maintaining the Division's management information systems which provide the 30,000 ft. view of the Division's overall workload and resource allocations. The Division required software development and maintenance services of six senior IT professionals to provide on-going support for significant software applications that support of mission critical services of ATR's operations.</p>
<p>Justice Management Division (JMD)</p>	<p>The JMD provides senior management officials with advice related to all matters pertaining to organization, management, and administration. The office of information resource management within JMD requires support in federal staff augmentation for Project Management Support, Network Services, Platform Services, Enterprise Mobility Services, Backup and Storage Support, Account Management Software Support, Mainframe Support, Information System Security Support, eDiscovery Service Support, End-user Device Management, Managed Service Desk, and Justice Communications System support.</p>
<p>Office of the Inspector General (OIG)</p>	<p>The mission of the Office of the Inspector General (OIG) is to detect and deter waste, fraud, abuse, and misconduct in the DOJ programs and personnel. There are three primary tasks associated with the task order. All are for unclassified and classified user applications and systems and will require in-depth knowledge of computer network/systems administration, applications support and configuration, and general IT assistance. Classified</p>

	systems support is limited as storage and applications are hosted by another DOJ component. User assistance to include file sharing, security, and file recovery may be required.
--	---

APPENDIX 4: Leidos, Inc.'s Response to the Draft Audit Report



August 14, 2023

David J. Gaschke
Regional Audit Manager
San Francisco Regional Audit Office
Office of the Inspector General
U.S. Department of Justice
90 7th Street, Suite 3-100
San Francisco, CA 94103

Dear Mr. Gaschke:

Please find the Leidos official responses below to the recommendations as set forth in the draft audit report (the "Report") of the ATF's Enterprise Standard Architecture contract awarded to Leidos in May 2020 (the "Contract"):

1. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
2. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
3. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
4. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
5. **Disagree, in part; Agree in part.** Leidos continues to submit timely, complete and accurate monthly reports which demonstrate adherence to all contract included key performance indicators ("KPIs"). The Contract does not contain KPIs for workstation patching nor Printer KPIs for replenishing printer cartridges for network printers and installing required IT security patches on printers. Therefore, such metrics were not included in monthly reports. In November 2021, Leidos was required to patch within 2 weeks pursuant to the CISA Binding Operational Directive without a Contract modification. ATF further accelerated the timeline to 7 days without a formal

modification to the contract. While Leidos continued to patch, Leidos was unable to meet the shortened timeframe. Leidos has since fully complied with all timely patching requirements to date. Leidos will work with ATF to ensure that the monthly status reports accurately and fully summarize its performance, technical progress and challenges as required.

6. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
7. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.
8. We believe the ATF is responsible to address this recommendation and we are not in a position to agree or disagree.

Kind Regards,



Adam Habibi
Leidos, Inc.
Director of Contracts

APPENDIX 5: The Bureau of Alcohol, Tobacco, Firearms and Explosives' Response to the Draft Audit Report



U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Assistant Director

Washington, DC 20226

www.atf.gov

700000:SRF
8310

MEMORANDUM TO: Assistant Director
(Office of Professional Responsibility and Security Operations)

FROM: Assistant Director
Office of Management / Science and Technology

SUBJECT: OIG Audit of ATF's Enterprise Standard Architecture V Task
Order Awarded to Leidos, Inc.

This memorandum responds to the recommendations contained in the Office of Inspector General's (OIG) draft report titled "Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Enterprise Standard Architecture V Task Order Awarded to Leidos, Inc." We welcome OIG's constructive comments and appreciate the opportunity to respond.

Recommendation 1: Involve all participating federal components in a review of its KPIs, revise those KPIs that need clarification, include disincentives where appropriate, retain supporting documentation on the development of the performance measures, and work with Leidos to modify the contract.

ATF concurs with this recommendation. ATF will create a working group, to include all participating federal components, to review and revise the current Key Performance Indicators (KPI's) and include disincentives, if appropriate. All supporting documentation will be retained by ATF following the guidelines set forth in ATF O 1340.5A, Records Management Program. After the KPI review, ATF will work with Leidos to modify the contract to incorporate the updated KPI's, if appropriate.

It is important to note that this modification to the contract must be bilateral and agreed upon by both parties before any KPI changes can be implemented. ATF expects to implement any changes to the

Assistant Director
(Office of Professional Responsibility and Security Operations)

KPI's during the "Option 2" contract renewal. The estimated completion time is the fourth quarter of Fiscal Year 2024.

Recommendation 2. Implement procedures to conduct periodic assessments to determine how current KPIs could be modified and whether new KPIs should be added to adequately address the government's need.

ATF concurs with this recommendation. ATF will implement a process to evaluate and revise the KPI's periodically to make them more realistic, relevant, or aligned with the current situation and objectives. If applicable, new KPI's will be created to reflect new priorities, challenges, or opportunities during the contract option year renewal process. The KPI's will be reviewed quarterly, as appropriate, to determine if the objectives and expectations are being achieved. The estimated completion time is the end of the fourth quarter of Fiscal Year 2024.

Recommendation 3. Develop procedures for future acquisitions that fully engage federal components in ensuring their concerns are adequately addressed prior to contract award and that includes controls to review and ensure the contract structure meets participating components' mission requirements.

ATF partially concurs with this recommendation. ATF did fully engage federal components in the early stages of the ESA V acquisition planning process. In addition to face-to-face discussions, ATF emailed each component requesting they provide the required services to be performed so that the appropriate Contract Line-Item Numbers (CLIN's) could be incorporated for each component. ATF advised component leadership that this vehicle would be structured differently than prior iterations of ESA, which would utilize a more detailed managed service approach.

Further, the Drug Enforcement Administration (DEA), the Antitrust Division (ATR) and the Justice Management Division (JMD) participated fully on the Technical Evaluation Panel (TEP). It was only after a change in leadership at these agencies that ATF was advised that the contract type and CLIN structure provided challenges to their mission requirements. Based upon the actions required to support the ESA V contract, ATF will limit component usage in future iterations of this contract.

Recommendation 4: Work with the participating components on evaluating options in modifying the option years of the ESA V task order to ensure the available CLINs and PWS interpretations are aligned and fully documented to minimize scope contentions and risk to component missions and objectives.

ATF partially concurs with this recommendation. Two of the agencies represented on the TEP (JMD and DEA), have completely and/or partially de-scoped services from ESA V. It is anticipated that JMD will de-scope the remainder of their services by the end of Option Year 1. ATR has already de-scoped services that have minimized prior scope contentions. ATF will engage the other components— the DOJ Criminal Division (CRM), the United States Trustee Program (USTP), and the Federal Bureau of Prisons (BOP)-- to ensure the CLIN's are aligned with their mission and objectives. The estimated completion time is the end of the third quarter of Fiscal Year 2024.

Assistant Director
(Office of Professional Responsibility and Security Operations)

Recommendation 5: Work with Leidos to ensure its monthly status reports accurately summarize its performance, technical progress, and challenges, as required.

ATF concurs with this recommendation. ATF will work with Leidos and the component users to ensure Leidos monthly status reports accurately summarize the performance, technical progress, and challenges. ATF will request explanation of the data sources, review all relevant background information used to produce the status reports and address inaccuracies in the data. The estimated completion time is the end of the second quarter of Fiscal Year 2024.

Recommendation 6: Implement procedures to ensure federal components review and identify inaccuracies and incompleteness in Leidos' monthly status reports.

ATF concurs with this recommendation. ATF will work with Leidos and the component users in the process of reviewing the monthly status reports. Component leadership will be engaged, if necessary.

Currently, the monthly status reports are component-based and sent only to those components. ATF will request the components provide detailed documentation on any inaccuracies and incompleteness of the report. Any concerns identified by the federal components will be provided to Leidos for immediate resolution. The estimated completion time is the end of the third quarter of Fiscal Year 2024.

Recommendation 7: Update their SOPs for security patch implementation to ensure reports and records are retained that track remediation efforts from start to finish.

ATF concurs with this recommendation. ATF will review and update the current Standard Operating Procedure (SOP) for Server Patch Maintenance. The SOP will cover the entire process for server patch maintenance, including patch requests, authorization, testing, completion, closure, and documentation of deviations and false positives. Patch implementation will be tracked through the ATF change management tool (ServiceNow).

A weekly change package will include the pre-implementation patch listing as well as post-implementation patch application reporting. This addition to the process will allow reconciliation and traceability of all approved patches applied throughout the patch change management lifecycle. The estimated completion time is the end of the first quarter of Fiscal Year 2024.

Recommendation 8: Implement procedures to perform forecasting and risk assessments with the program owners during the acquisition planning phase and throughout the task order performance, in compliance with the FAR.

ATF concurs with this recommendation in part. For future acquisition planning, ATF will evaluate risks per FAR 7.105(a)(7), Contents of Written Acquisition Plans. Under this section of the FAR, acquisition plans should discuss the technical, cost, and schedule risks and describe what efforts are planned or underway to reduce risk and the consequences of failure to achieve goals. If concurrency

Assistant Director
(Office of Professional Responsibility and Security Operations)

of development and production is expected, acquisition plans will discuss its effects on cost and schedule risks.

Please let me know if we can be of further assistance on this or any other matter.

**FRANCIS
FRANDE**  Digitally signed by
FRANCIS FRANDE
Date: 2023.08.18
10:38:51 -04'00'

Francis Frande

**ROGER
BEASLEY**  Digitally signed by
ROGER BEASLEY
Date: 2023.08.18
12:03:59 -04'00'

Roger Beasley

APPENDIX 6: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

The OIG provided a draft of this audit report to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and Leidos, Inc. (Leidos). Leidos' response is incorporated in Appendix 4, and ATF's response is incorporated in Appendix 5 of this final report. Since the audit recommendations were directed at ATF, Leidos was not required to provide the OIG with a response. However, Leidos provided us with a response indicating that it partially agreed with recommendation 5. For the remaining recommendations, Leidos stated that it was not in a position to agree or disagree as it believed ATF was responsible to address them. ATF concurred with 5 of our recommendations, partially concurred with the remaining 3 recommendations, and discussed the actions it will implement in response to our findings. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the response and summary of actions necessary to resolve the report.

Recommendations for ATF:

- 1. Involve all participating federal components in a review of its KPIs, revise those KPIs that need clarification, include disincentives where appropriate, retain supporting documentation on the development of the performance measures, and work with Leidos to modify the contract.**

Resolved. ATF concurred with our recommendation. ATF stated in its response that ATF will create a working group, to include all participating federal components, to review and revise the current Key Performance Indicators (KPI) and include disincentives, if appropriate. All supporting documentation will be retained by ATF following the guidelines set forth in ATF O 1340.5A, Records Management Program. After the KPI review, ATF will work with Leidos to modify the contract to incorporate the updated KPIs, if appropriate. ATF added that a modification to the contract must be bilateral and agreed upon by both ATF and Leidos. ATF expects to implement any changes to the KPIs during the Option 2 contract renewal and it anticipates completing this corrective action in the fourth quarter of Fiscal Year (FY) 2024. As a result, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has reviewed ESA V's KPIs with all participating federal components, revised those KPIs that need clarification, has included disincentives where appropriate, retained supporting documentation on the development of the performance measures, and worked with Leidos to modify the contract.

- 2. Implement procedures to conduct periodic assessments to determine how current KPIs could be modified and whether new KPIs should be added to adequately address the government's need.**

Resolved. ATF concurred with our recommendation. ATF stated in its response that it will implement a process to periodically evaluate and revise the KPIs to make them more realistic, relevant, or aligned with the current situation and objectives. If applicable, the new KPIs will be

created to reflect new priorities, challenges, or opportunities during the contract option year renewal process. Further, the KPIs will be reviewed quarterly, as appropriate, to determine if the objectives and expectations are being achieved. ATF anticipates completing its corrective action by the end of the fourth quarter of FY 2024. As a result, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has implemented procedures to conduct periodic assessments to determine how current KPIs could be modified and whether new KPIs should be added to adequately address the government's need.

3. Develop procedures for future acquisitions that fully engage federal components in ensuring their concerns are adequately addressed prior to contract award and that includes controls to review and ensure the contract structure meets participating components' mission requirements.

Resolved. ATF stated in its response that it partially concurred with our recommendation. In its response, ATF stated that it fully engaged federal components in the early stages of the ESA V acquisition planning process, citing that this included face-to-face discussions and ATF emails to each component requesting they provide the required services to be performed so that the appropriate Contract Line-Item Numbers (CLIN) could be incorporated for each component. ATF also stated that it advised component leadership that this vehicle would be structured differently than prior iterations of ESA, which would utilize a more detailed managed service approach. Further, ATF asserted in its response that the Drug Enforcement Administration (DEA), the Antitrust Division (ATR), and the Justice Management Division (JMD) participated fully on the Technical Evaluation Panel (TEP), but after changes in leadership at these agencies, ATF was advised that the contract type and CLIN structure presented challenges to their mission requirements. ATF further stated that based upon the actions required to support the ESA V contract, ATF will limit component usage in future iterations of this contract.

Our audit results revealed that ATF did not fully address JMD's concerns about the firm fixed price (FFP) contract type before awarding the contract. As we discussed in the report, approximately 3 months prior to the ESA V task order award, JMD expressed concerns to ATF's contracting officer that there were no suitable T&M CLINs to which JMD could subscribe, and the majority of their needed services fell under the FFP CLINs, which did not lend itself to modifications and flexibility. The contracting officer did not respond to JMD's concerns. As we highlighted in our report, this lack of flexibility led to the need for a contract modification to move network operations contract personnel from an FFP CLIN to a more flexible T&M CLIN, resulting in increased costs to JMD. This exemplifies the need for ATF to develop procedures for future acquisitions that ensure components' concerns are adequately addressed prior to contract award and ensure that the contract structure meets participating components' mission requirements. While ATF indicated in its response that this will not be necessary for the next solicitation for these services, ATF's ESA V task order's period of performance ends in April 2029. Therefore, it may not be the decision of ATF leadership in 2029 to limit the ESA program's participation. Thus, implementing procedures to ensure ATF's contracts are

structured to meet its customers' mission requirements provides a more enduring solution for any future enterprise-wide procurements beyond ATF's ESA V task order.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

Given ATF's general recognition that it is important to engage other federal components involved in its ESA contract, this recommendation is resolved. This recommendation can be closed when ATF develops and formalizes procedures covering all future acquisitions that involve external components, to include fully engaging components to ensure their concerns are adequately addressed prior to contract award and that includes controls to review and ensure the contract structure meets participating components' mission requirements.

- 4. Work with the participating components on evaluating options in modifying the option years of the ESA V task order to ensure the available CLINs and PWS interpretations are aligned and fully documented to minimize scope contentions and risk to component missions and objectives.**

Resolved. ATF stated in its response that it partially concurred with our recommendation. ATF also stated that two of the agencies represented on the Technical Evaluation Panel (JMD and DEA) have completely or partially de-scoped services from ESA V; ATF anticipates that JMD will de-scope the remainder of its services by the end of Option Year 1; and ATR has already de-scoped services that have minimized prior scope contentions. ATF stated that it will engage the other components—the Criminal Division, the United States Trustee Program, and the Federal Bureau of Prisons—to ensure that the CLINs are aligned with their mission and objectives. ATF anticipates completing its corrective action by the end of the third quarter of FY 2024. As a result of these planned actions, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has worked with the participating components on evaluating options in modifying the option years of the ESA V task order to ensure that the available CLINs and PWS interpretations are aligned and fully documented to minimize scope contentions and risk to component missions and objectives.

- 5. Work with Leidos to ensure its monthly status reports accurately summarize its performance, technical progress, and challenges, as required.**

Resolved. ATF concurred with our recommendation. ATF stated in its response that it will work with Leidos and the component users to ensure Leidos monthly status reports accurately summarize performance, technical progress, and challenges. ATF will request explanation of the data sources, review all relevant background information used to produce the status reports, and address inaccuracies in the data. ATF anticipates completing its corrective action by the end of the second quarter of FY 2024. As a result, this recommendation is resolved.

In its response, Leidos stated that it agreed, in part, and disagreed, in part, with our audit recommendation. Leidos stated that it continues to submit timely, complete, and accurate monthly reports which demonstrate adherence to all contract requirements including KPIs. According to Leidos, the contract does not contain KPIs for workstation patching or replenishing printer cartridges for network printers and installing required IT security patches on printers. Thus, such metrics were not included in monthly reports. Leidos also stated that in November 2021 it was required to patch within 2 weeks pursuant to the Cybersecurity and Infrastructure Security Agency Binding Operational Directive without a contract modification and that ATF further accelerated the timeline to 7 days without a formal modification to the contract. While Leidos continued to patch, it reported that it was unable to meet the shortened timeframe. Leidos stated that it has since fully complied with all timely patching requirements to date. Leidos stated that it will work with ATF to ensure that the monthly status reports are accurate and fully summarize its performance, technical progress, and challenges as required.

As we discussed in the report, the ESA V PWS required Leidos to provide federal components with monthly status reports that contain their compliance levels and briefly summarize management and technical progress and challenges. We determined that Leidos did not provide an accurate self-assessment of its performance when it did not include its technical progress and challenges in the two monthly reports we sampled. Specifically, Leidos was having frequent and urgent discussions with ATF in November 2021 regarding the challenges of complying with the Department OCIO's mandates on security patching. Also, Leidos' monthly status report did not reflect it failing to meet the Department OCIO's August 21, 2020, security patch deadline, leaving ATR's 84 assets unpatched as of August 27, 2020. Although the task order QASP did not include KPIs for workstations patching, Leidos did not discuss its progress and challenges with meeting the Department OCIO's patch timeframes, as required by the PWS. None of these findings are associated with the printer patches and cartridges that Leidos cited in its response. As summarized in Table 3 of the report, the government drafted Letters of Concern regarding Leidos' performance issues.

This recommendation can be closed when we receive evidence that ATF has worked with Leidos to ensure its monthly status reports accurately summarize its performance, technical progress, and challenges, as required.

6. Implement procedures to ensure federal components review and identify inaccuracies and incompleteness in Leidos' monthly status reports.

Resolved. ATF concurred with our recommendation. ATF stated in its response that it will work with Leidos and the component users in the process of reviewing the monthly status reports. Component leadership will be engaged, if necessary. Currently, the monthly status reports are component-based and sent only to those components. ATF will request that the components provide detailed documentation on any inaccuracies and incompleteness of the report. Any concerns identified by the federal components will be provided to Leidos for immediate resolution. ATF anticipates completing its corrective action by the end of the third quarter of FY 2024. As a result, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has implemented procedures to ensure federal components review and identify inaccuracies and incompleteness in Leidos' monthly status reports.

7. Update their SOPs for security patch implementation to ensure reports and records are retained that track remediation efforts from start to finish.

Resolved. ATF concurred with our recommendation. ATF stated in its response that ATF will review and update the current Standard Operating Procedure (SOP) for Server Patch Maintenance. The SOP will cover the entire process for server patch maintenance, including patch requests, authorization, testing, completion, closure, and documentation of deviations and false positives. Patch implementation will be tracked through ATF's change management tool. A weekly change package will include the pre-implementation patch listing as well as post-implementation patch application reporting. This addition to the process will allow reconciliation and traceability of all approved patches applied throughout the patch change management lifecycle. ATF anticipates completing its corrective action by the end of the first quarter of FY 2024. As a result, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has updated their SOPs for security patch implementation to ensure reports and records are retained for tracking remediation efforts from start to finish.

8. Implement procedures to perform forecasting and risk assessments with the program owners during the acquisition planning phase and throughout the task order performance, in compliance with the FAR.

Resolved. ATF stated that it concurred with this recommendation in part. ATF stated in its response that, for future acquisition planning, ATF will evaluate risks per FAR 7.105(a)(7), Contents of Written Acquisition Plans, which states that acquisition plans should discuss the technical, cost, and schedule risks and describe what efforts are planned or underway to reduce risk and the consequences of failure to achieve goals. ATF further stated that, if concurrency of development and production is expected, its acquisition plans will discuss its effects on cost and schedule risks. As a result of ATF's planned actions, this recommendation is resolved.

Leidos did not agree or disagree with this recommendation as Leidos believed that ATF was responsible for addressing this recommendation.

This recommendation can be closed when we receive evidence that ATF has implemented

procedures to perform forecasting and risk assessments with the program owners during the acquisition planning phase and throughout the task order performance, in compliance with the FAR.