



UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL

Assessment of the United States Capitol Police Use of Avue Digital Services System

Report Number OIG-2019-08

March 2019

~~**Report Restriction Language**~~

~~**Distribution of this Document is Restricted**~~

~~This report may contain sensitive law enforcement information and/or is part of the deliberative process privilege. This is the property of the Office of Inspector General and is intended solely for the official use of the United States Capitol Police, the Capitol Police Board, or any agency or organization receiving the report directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the United States Capitol Police or the Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~



INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports OIG prepares periodically as part of its oversight responsibility with respect to the United States Capitol Police (USCP) to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office or function under review. Our work was based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG and discussed in draft with those responsible for implementation. It is my hope that the recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to those contributing to the preparation of this report.

Michael A. Bolton,
Inspector General

TABLE OF CONTENTS

	<u>Page</u>
Abbreviations and Acronyms	iii
Executive Summary	1
Background	2
Objectives, Scope, and Methodology	4
Results	6
Monitoring of the Avue Contract	6
Controls to Ensure the Integrity of the Avue Data	8
Compliance with Laws, Regulations, and Guidance	9
Appendices	10
Appendix A – List of Recommendations	11
Appendix B – Department Comments	12

Abbreviations and Acronyms

Avue Digital Services System	Avue
Calendar Year	CY
Contracting Officer's Representative	COR
Federal Risk and Authorization Management Program	FedRAMP
Government Accountability Office	GAO
Lieutenant Voluntary Reassignment Program	LVRP
National Finance Center	NFC
National Institute of Standards and Technology	NIST
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
Office of Management and Budget	OMB
Officer Voluntary Reassignment Process Module	OVRP Module
Officer Voluntary Reassignment Program	OVRP
Sergeant Voluntary Reassignment Program	SVRP
Service Level Agreement	SLA
Software-as-a-Service	SaaS
Special Publication	SP
Statement on Standards for Attestation Engagements 18	SSAE 18
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

Congress passed the *E-Government Act* (Public Law 107-347), dated December 17, 2002, to promote use of the internet and electronic Government services, make the Federal Government more transparent and accountable, and increase operational efficiencies by moving away from paper-heavy processes. As cloud computing has emerged as an important platform in recent years, offering organizations improved operational efficiencies and cost savings, the Office of Management and Budget released its *25 Point Implementation Plan to Reform Federal Information Technology Management*, dated December 9, 2010, to help the Federal Government achieve benefits. The implementation plan required that agencies immediately shift to a “Cloud First” policy and default to cloud-based services whenever a secure, reliable, and cost-effective cloud option existed.

As part of its efforts to transition from a manual to an automated process, the United States Capitol Police (USCP or the Department) implemented a Software-as-a-Service (SaaS)¹ cloud-based Human Capital Management and Operations Management platform called Avue Digital Services System (Avue) in September 2005. Avue offered 12 integrated, web-based modules within its automated system for various workforce management processes, and USCP has subscribed to multiple modules over the life of the contract. The Department has used Avue for its Officer Voluntary Reassignment Program (OVRP), Sergeant Voluntary Reassignment Program, and Lieutenant Voluntary Reassignment Program since 2012.

In accordance with our *Annual Performance Plan Fiscal Year 2019*, dated October 2018, the Office of Inspector General (OIG) assessed Avue. Our objectives were to determine if the Department (1) appropriately monitored the Avue contract, (2) established effective controls that ensured the integrity of Avue data, and (3) complied with laws, regulations, and guidance. Our scope included controls, processes, and operations during calendar year 2018.

The Department did not adequately monitor its contract with Avue and ensure the security controls for the cloud service provider complied with USCP, Federal Information Security Management Act, and National Institute of Standards and Technology guidelines. As well, the Department could have improved Avue services by requesting a system change that included a validation check within Avue. Such a change would have ensured that OVRP applicants correctly filled in the required fields and provided email confirmation and copy of the transaction. Applying such best practices would have improved Department monitoring of the SaaS contract and ensured both the integrity and security of the employee data.

¹ In a SaaS platform, the vendor provides and manages all software and hardware.

The Department can improve data security, compliance with best practices, and enhance customer service. OIG made two recommendations as shown in Appendix A.

On March 12, 2019, OIG provided a draft report to Department officials for comment. We incorporated the Department's comments as applicable and attached the response to the report in its entirety in Appendix B.

Background

The United States Capitol Police (USCP or the Department) Office of Human Resources (OHR) awarded a contract in 2005 for implementation of a Software-as-a-Service (SaaS) cloud-based Human Capital Management and Operations Management platform, Avue Digital Services System (Avue), as part of an effort to reengineer its manual workflow process. In a SaaS platform, the vendor provides and manages all software and hardware.

Avue offered 12 integrated, web-based modules within its automated system related to various workforce management processes. In the base year of the contract, USCP purchased only the Recruitment, Retention, and Staffing Module—a module used for both civilian and sworn staffing—along with the base operating system. During the following year as it continued to reengineer its processes and move toward automation, OHR purchased two additional modules—the Performance Management Module and the Recruitment, Hiring, Placement, Retention, and Assessment Module.

In 2008, the Department's voluntary reassignment process transitioned from a manual process to an automated process. Avue developed an automated tool that integrated with data from the National Finance Center (NFC) and USCP specific requirements such as the number of allocated positions per bureau or division, shifts, and seniority. The tool became an official Avue module called the "Officer Voluntary Reassignment Process" (OVRP Module). In 2009, OHR purchased another two modules—the Injury Compensation Program and Case Management Module and Enterprise Learning Module—to support its Workers' Compensation Program and Training Services Bureau, respectively.

Reduced funding in 2012, however, dictated that USCP reevaluate its programs. Of the six modules to which USCP subscribed, the Department elected to continue with only the OVRP Module, which included the Officer Voluntary Reassignment Program (OVRP), Sergeant Voluntary Reassignment Program (SVRP), and Lieutenant Voluntary Reassignment Program (LVRP). Since then, the Department has used Avue to assist with meeting the staffing needs of the Department.

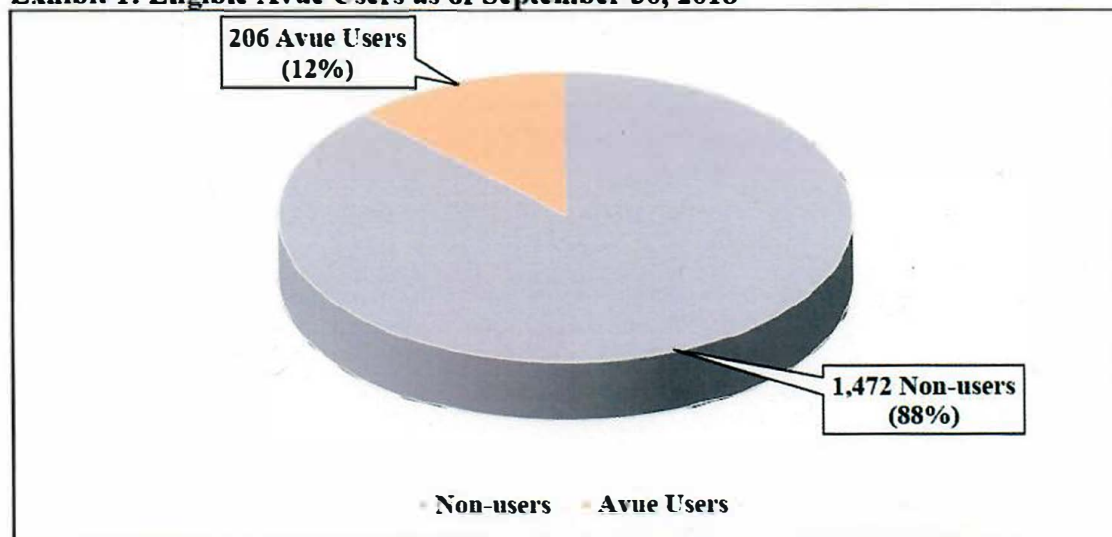
USCP officers below the rank of Sergeant who seek voluntary reassignment apply during an open season through Avue's OVRP Module. The Chief of Police is responsible for

designating the open seasons, which can last up to 30 days and take place twice each year. Officers submit their requests for reassignment with Avue. The requests consist of assignment data and reassignment preferences. Avue preloads information from NFC so that the fields (except reassignment preferences) are prepopulated when users log in. It is an officer's responsibility to ensure that information is current and complete.

Applicants may select up to five reassignment choices listed in order of preference and are able to change the preferences at any time during the open season. The Department bases reassignment priority on (1) the needs of the Department, (2) personal preference, and (3) seniority. After open season closes, a Human Resource Specialist validates applicant information prior to processing of applications. Once validation is complete, Avue generates a processing report in Excel showing each applicant's reassignment preferences.

According to documentation OHR provided, as of September 30, 2018, the Department had 1,925 sworn personnel, 1,678 (87 percent) of whom were eligible to apply for the OVRP and sign up for Avue. As of September 30, 2018, there were 206 active Avue accounts. See Exhibit 1 for the composition of eligible Avue users.

Exhibit 1: Eligible Avue Users as of September 30, 2018



Source: Office of Inspector General (OIG) generated from OHR data as of September 30, 2018.

During Calendar Year (CY) 2018, the Department held two open seasons for its OVRP—one in June and another in December. Open seasons for SVRP and LVRP occur only once every year or two, based on the Department needs. The process for SVRP and LVRP is the same as that of OVRP. Through the processes, Sergeants and Lieutenants can request shift preferences and reassignment options. The last open season for SVRP and LVRP took place in November 2017.

According to documentation OHR provided, a total of 219 officers applied for reassignment during the June 2018 open season, 101 (46 percent) of whom were approved for reassignment. During the December 2018 open season, a total of 183 applicants applied for OVRP, and 106 (58 percent) applicants were selected for reassignment. See Table 1 displaying OVRP application results.

Table 1: OVRP Application Results

OVRP	Reassigned		Not Reassigned		Total
June 2018	101	46%	118	54%	219
December 2018	106	58%	77	42%	183

Source: OIG generated from OHR data during CY 2018.

OBJECTIVES, SCOPE, AND METHODOLOGY

OIG objectives were to determine if the Department (1) appropriately monitored the Avue contract, (2) established effective controls that ensured the integrity of the Avue data, and (3) complied with laws, regulation, and guidance. Our scope included controls, processes, and operations during CY 2018.

To accomplish our objectives, we interviewed USCP officials to gain an understanding of the Avue in the following areas:

- Contract requirements
- Data flow process to include such stages as: account set up, data entry, submission, receipt, and review
- Results communication
- OHR's responsibilities
- Controls related to data integrity
- Activities for monitoring the contract with Avue

We also reviewed the following laws, guidance, and industry best practices:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013 (included updates as of January 22, 2015)

- Government Accountability Office (GAO) *Standards for the Internal Controls in the Federal Government*, GAO-14-704G, dated September 2014
- Directive [REDACTED], dated March 3, 2014
- Office of Management and Budget (OMB) Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, dated December 8, 2011
- OMB 25 Point Implementation Plan to Reform Federal Information Technology Management, dated December 9, 2010
- E-Government Act of 2002 (Public Law 107-347), dated December 17, 2002

As a legislative branch entity, many laws and regulations that apply to executive branch agencies do not apply to USCP. We believe, however, that those laws and regulations represent appropriate guidance and industry best practices for USCP.

To determine if the Department appropriately monitored the contract with Avue, we examined the contract and assessed whether Avue met contract requirements. We interviewed Department officials to further our understanding of the Avue process.

To evaluate whether the Department established effective controls that would ensure the integrity of the Avue data, we conducted a walkthrough of the OVRP process to identify data entry points, relevant internal controls, and associated risks. Additionally, we reviewed a list of Avue users and user categories with security privileges for each. We also reviewed Avue processing reports and helpdesk tickets to identify possible risk indicators for data integrity.

To assess the Department's compliance with laws, regulations, and guidance, we requested a copy of the service level agreement (SLA) and Avue's Statement on Standards for Attestation Engagements 18 (SSAE 18) report. We also inquired about the Department's procedures for security control compliance as they related to the Avue process. We used the GAO, OMB, and NIST guidance as best practices.

We conducted this assessment in Washington, D.C., from January to February 2019. We did not conduct an audit, the objective of which would be the expression of an opinion on Department programs. Accordingly, we do not express such an opinion. OIG did not conduct this assessment in accordance with generally accepted government auditing standards. Had we conducted an audit and followed such standards, other matters might have come to our attention.

On March 12, 2019, we provided a draft copy of this report to Department officials for comment. A list of recommendations is detailed in Appendix A. We incorporated Department comments as applicable and attached the response to the report in its entirety as Appendix B.

RESULTS

The USCP Contracting Officer's Representative (COR) did not adequately monitor the contract with Avue to ensure that security controls the cloud service provider used complied with USCP, Federal Information Security Management Act, and NIST guidelines. Because of the lapse in monitoring, the Department did not assess the security of Avue. During discussions with Department officials, an opportunity for improving Avue customer service was identified. One source of applicant complaints was because applicants leave the "selection" field blank. The Department can enhance the Avue service by requesting system changes such as a validation check within Avue and a confirmation email that includes the details of the OVRP transaction.

Monitoring of the Avue Contract

The USCP COR did not adequately monitor the contract for Avue services. Section C.7.1 of the contract for Avue services concerning data security requirements states, "USCP specific data will include sensitive personnel information (e.g., SSN [social security number]), which must be stored in a secure environment that meets or exceeds USCP, FISMA [Federal Information Security Management Act], and NIST guidelines." The contract further states, "The USCP Office of Information Systems (OIS) Information Systems Security Specialist / Officer must certify all USCP agency personnel data stored at any remote contractor site is secure." The COR did not have information related to the requirement.

The contract predated the current OIS staff, and OIS was not aware of the contract clause requiring an OIS certification. NIST SP 800-53, Revision 4, Control SA-9 states,

... the organization requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

The COR did not keep OIS informed and did not ensure that the vendor met OIS data security requirements, which would have included review of SSAE 18 reports² and the Federal Risk and Authorization Management Program (FedRAMP)³ security authorization package. USCP officials stated that not only was USCP not reviewing SSAE 18 reports, but it also did not have an SLA in place and did not review the FedRAMP security authorization package. Without an SLA defining the responsibilities of each party, the level of service expected, and performance metrics, the Department could not objectively assess the performance and security level of Avue.

Conclusions

The Department did not monitor contractor requirements for data security and privacy. The Department did not have an SLA, and the Department did not monitor compliance of security controls for the cloud service provider by reviewing the SSAE 18 reports or the FedRAMP security authorization package. Without reviewing the FedRAMP package and SSAE 18 reports for cloud-based services, the Department may not have been aware of potential weaknesses in their control environment—weaknesses that could have affected the confidentiality, integrity, and availability of Avue. As a result, employee data was at risk. Thus, OIG makes the following recommendation:

Recommendation 1: We recommend that the United States Capitol Police (USCP) document and implement a procedure for identifying all information system service contracts that should have a service level agreement, and if the contract properly defines each party's responsibilities. Additionally, for each information system service contract, document the applicability of Federal Risk and Authorization Management Program security authorization packages and third party Statement on Standards for Attestation Engagements 18 reports. Any information system service contract should be provided to the USCP Office of Information Systems.

Controls to Ensure the Integrity of the Avue Data

Opportunity to Improve Service

Avue did not have a validation check that forced officers to complete all of the necessary parts of the OVRP application before allowing submission. OHR representatives stated

² Organizations review SSAE 18 reports, which provide information about the internal controls and security practices at a service organization, to monitor security control compliance by external service providers.

³ FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services that is mandatory for Federal Agency cloud deployments and service models at the low, moderate, and high risk impact levels.

that OVRP applicants occasionally left selection fields blank when filling out reassignment forms. Although Avue generated a confirmation email to the applicant about an edit, the confirmation did not provide specifics for the change. When an officer's application did not specify priority reassignment choices, Avue automatically excluded the applicant from reassignment opportunity. That action caused an officer to be unsatisfied with the process. The GAO-14-704G states,

Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results... External parties can also help management identify issues in the internal control system. For example, complaints from the general public and regulator comments may indicate areas in the internal control system that need improvement. Management considers whether current controls address the identified issues and modifies controls if necessary.

According to officials, OHR did not review submissions until after the open season closed. Although applicants were able to print a copy of a request during open season, many officers did not keep a copy for their records. And although applicants received an email confirming submission of a request, the email did not include the details of the request. According to officials, the officers generally believed they successfully completed the process only to find out later that their applications were incomplete. With the system closed and without evidence, the applicants had no recourse. Such experience could hurt morale when officers believe that they requested a transfer they do not receive. USCP should request that Avue improve the process by adding validation edits to the submission form and modifying the confirmation email to include details of the OVRP application.

Conclusions

Avue did not have a validation check feature that would have ensured officers submitted necessary parts of the OVRP application. Without a validation check feature in the program preventing submission of incomplete applications, the system was susceptible to submission of incomplete reassignment choices. This has led to complaints by officers who did not properly submit their reassignment choices and claimed data integrity errors and ineffective administration of the OVRP process. OIG, therefore, makes the following recommendation:

Recommendation 2: We recommend that the United States Capitol Police coordinate with the Avue vendor and request a system change that includes a validation check within Avue to ensure that Officer Voluntary Reassignment Program applicants fill in all of the required fields correctly prior to submission and to provide applicants a copy of the transaction in an email confirmation.

Compliance with Laws, Regulations, and Guidance

Lack of Service Level Agreement

The Department did not have an SLA and did not review the FedRAMP security authorization package or SSAE 18 reports. Those reports are required by NIST SP 800-53.

Conclusions

The Department did not have an SLA and did not monitor the cloud service provider's security control compliance by reviewing SSAE 18 reports or FedRAMP security authorization package. Without review of the FedRAMP security authorization package and SSAE 18 reports for security assessment and continuous monitoring of the cloud-based services, USCP may not have been aware of potential weaknesses in its control environment that could have affected the confidentiality, integrity, and availability of Avue and may put employee data at risk. OIG made Recommendation 1 as stated above in the section titled *Monitoring of the Avue Contract*.

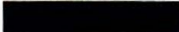
APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police (USCP) document and implement a procedure for identifying all information system service contracts that should have a service level agreement, and if the contract properly defines each party's responsibilities. Additionally, for each information system service contract, document the applicability of Federal Risk and Authorization Management Program security authorization packages and third party Statement on Standards for Attestation Engagements 18 reports. Any information system service contract should be provided to the USCP Office of Information Systems.

Recommendation 2: We recommend that the United States Capitol Police coordinate with the Avue vendor and request a system change that includes a validation check within Avue to ensure that Officer Voluntary Reassignment Program applicants fill in all of the required fields correctly prior to submission and to provide applicants a copy of the transaction in an email confirmation.

DEPARTMENT COMMENTS

	UNITED STATES CAPITOL POLICE	Phone: 202-224-2800
	OFFICE OF THE CHIEF 119 D STREET, NE WASHINGTON, DC 20510-7218	
	March 20, 2019	
		COP 190010
MEMORANDUM		
TO:	Mr. Michael A. Bolton Inspector General	
FROM:	Matthew R. Verderosa Chief of Police	
SUBJECT:	Response to Office of Inspector General draft report <i>Assessment of the United States Capitol Police Use of Avue Digital Services System</i> (Report No. OIG-2019-08)	
The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of Inspector General's (OIG) draft report <i>Assessment of the United States Capitol Police Use of Avue Digital Services System</i> (Report No. OIG-2019-08). The Department generally agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon current policies and procedures within the Department. The Department will assign Action Plans to appropriate personnel regarding each recommendation in effect to achieve long term resolution of these matters. Thank you for the opportunity to respond to the OIG's draft report. Your continued support of the women and men of the United States Capitol Police is appreciated. Very respectfully,  Matthew R. Verderosa Chief of Police cc: Steven A. Sund, Assistant Chief of Police Richard L. Braddock, Chief Administrative Officer  USCP Audit Liaison Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.		

This page intentionally left blank

CONTACTING THE OFFICE OF INSPECTOR GENERAL

Success of OIG mission to prevent fraud, waste, abuse, or mismanagement depends on the cooperation of employees and the public. There are several ways to report questionable activity.

Call us at 202-593-1972 or toll-free at 866-906-2446. A confidential or anonymous message can be left 24 hours a day/7 days a week.

Toll-Free - 1-866-906-2446



Write us:

***United States Capitol Police
Attn: Office of Inspector General
499 South Capitol St. SW, Suite 345
Washington, DC 20003***



Or visit us:

***499 South Capitol Street, SW, Suite 345
Washington, DC 20003***



You can also contact us by email at:

**When making a report, convey as much information as possible such as:
Who? What? Where? When? Why? Complaints may be made anonymously or you may
request confidentiality.**

Additional Information and Copies:

To obtain additional copies of this report, call OIG at 202-593-4201.

