DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

OFFICE OF INFORMATION AND TECHNOLOGY

VA Applications Lacked Federal Authorizations, and Interfaces Did Not Meet Security Requirements

REVIEW | REPORT #20-00426-02 | DECEMBER 2, 2021

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

As part of its day-to-day operations, VA must handle vast amounts of sensitive data, including veterans' healthcare information, through a number of cloud-based applications. As a solution to this type of data management problem, cloud computing allows ubiquitous, convenient, on-demand network access to information, but with easy access comes potential security risks. To mitigate those risks, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP), which promotes the adoption of secure cloud services by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. FedRAMP policies provide a cost-effective, risk-based approach for adopting and using cloud services, and VA is required to follow FedRAMP policies, procedures, and guidelines in all cloud deployment scenarios. "FedRAMP authorized" refers to reusable authorizations for cloud products and services that have been predetermined to meet baseline security requirements for federal agency use. However, VA still requires approval for operation on its network.

In April 2019, the VA Office of Inspector General (OIG) received allegations that a division in VA's Office of Information and Technology (OIT)—Project Special Forces (PSF)—was not following FedRAMP policies or VA policy for deploying software-as-a-service (SaaS) applications.[1] The specific allegations concerned unauthorized applications and those applications managed outside established lines of authority:

1. **Unauthorized applications.** OIT allegedly allowed SaaS applications that were not FedRAMP authorized to be used on VA's network, and PSF allegedly advocated the use of nine unauthorized SaaS applications (including Dropbox, Google Drive, iCloud, GitLab, SlideShare, Evernote, Basecamp, Datadog, and PagerDuty), putting VA and veterans' data at risk.[2]
2. **Improperly managed applications.** PSF allegedly was developing VA applications for the cloud that were managed outside the VA Enterprise Cloud group, which is responsible for the utilization of all VA cloud assets.[3] While evaluating the merit of this

[1] OMB, Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; VA Directive 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016. According to OIT staff, PSF assists in approving SaaS applications for use on VA's network, but OIT grants the authority to operate and is responsible for deploying the applications on the network. Therefore, despite the complainant's wording, in this report the review team substitutes "OIT" in discussing all but the development and advocacy mentioned in the allegations.

[2] SaaS applications are hosted and managed by a third-party software cloud service provider. They allow VA to use the service without having to maintain the system or manage the infrastructure.

[3] Managing applications and interfaces outside the purview of this group may result in unsecure and inconsistent cloud functionality.

allegation, the OIG also assessed whether PSF developed cloud-based applications and services in compliance with VA security standards.

Federal and VA security standards are intended to protect data from unauthorized use. If OIT does not comply with these standards, VA and veterans' data could be unnecessarily compromised.

What the Review Found

The OIG substantiated that OIT was not fully following FedRAMP policies or VA policy for SaaS applications (which was part of the first allegation). Specifically, OIT did not adhere to FedRAMP requirements when it granted security authorizations and the authority to operate on the VA network for applications that lacked prior FedRAMP authorization.[4] In examining the second part of allegation 1, the OIG found no evidence that PSF advocated for the nine applications cited by the complainant. However, eight of the nine applications were in use on the VA network—some without FedRAMP or VA authorization. The OIG also determined that seven of the SaaS applications were not granted authority to operate.[5] This noncompliance occurred because OIT allowed some partners that did not meet VA security baselines to use external connections to VA's network. OIT also used legacy SaaS applications it considered low risk while still in the authorization to operate process. Finally, certain SaaS applications were allowed through the VA firewall without assessing their risk.

Some of these issues have since been addressed. In January 2021, OIT updated security for external partner connections to meet security baselines—remediating three of the eight applications. In June 2021, one application was configured to remove access through VA's firewall.

As to allegation 2, the OIG did not substantiate that PSF-developed interfaces were improperly managed outside the VA Enterprise Cloud group. PSF's application development was limited to five Lighthouse application programming interfaces, which were hosted on the VA Enterprise Cloud and managed by the Enterprise Cloud Solutions Office, consistent with established lines of authority. Application programming interfaces allow third parties to "plug into" the VA to send and retrieve data. This capability simplifies and streamlines veteran access to VA data and

[4] VA Directive 6517; VA Handbook 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016. VA Directive 6517 requires VA to follow FedRAMP policies, procedures, and guidelines in all cloud deployment scenarios. VA Handbook 6517 states that VA is responsible for granting authority to operate. In addition, it states that OIT is responsible for ensuring VA systems that have undergone an assessment and authorization are continuing to operate at their authorized level of risk. According to the handbook, an authority to operate is "[t]he official management decision given by a senior organizational official, after completing a security assessment, to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls."

[5] Appendix A details the review scope and methodology.

services while reducing administrative burden. The review team did find, however, that PSF did not follow VA security requirements in developing the interfaces.

OIT Allowed the Use of Unauthorized Software

During the review, the OIG also determined that, as of March 9, 2020, OIT had approved the use of 19 SaaS applications (distinct from the nine applications identified in allegation 1 above) on VA's networks with assistance from PSF.[6] Three of those applications were approved to operate on VA's network without the required FedRAMP authorization. One of these applications still lacked FedRAMP authorization as of July 2021.

For the three noncompliant SaaS applications, OIT personnel gave the following reasons for not meeting federal authorization requirements:

- There was no formal OIT process for granting authority to operate until April 2019. After the process was established, the review team did not find instances of VA improperly granting an authority to operate before FedRAMP authorization.
- OIT staff misunderstood the FedRAMP authorization requirements for SaaS applications containing data classified as less sensitive.[7]

Applications that are on the network but cannot or do not meet FedRAMP security authorization requirements must be listed in an annual certification letter from VA to the Federal Chief Information Officer, along with the appropriate rationale and proposed mitigation plan.[8] By not meeting federal authorization requirements, OIT managers cannot ensure that the security controls comply with federal standards and will adequately protect veterans' personally identifiable information and protected health information from unauthorized access.

[6] OIT staff stated that assistance consists of helping would-be business owners complete procurement paperwork, providing acquisition language for service line agreements, and working collaboratively with the SaaS cloud service providers to complete FedRAMP documentation. Because the allegation specifically mentioned PSF, the OIG reviewed only SaaS applications with which PSF staff said they assisted.

[7] National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," *Federal Information Processing Standard Publications (FIPS PUBS) 199*, February 1, 2004. Here, "less sensitive" refers to SaaS applications with a data categorization of low impact, as VA applies FIPS Publication 199. These categorizations are based on the potential effect on an organization should the data be compromised. OIT staff wrongly believed that a formal FedRAMP authorization was not required.

[8] OMB, Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments."

Application Programming Interfaces Were Managed by the Correct Group, but OIT Did Not Meet VA Security Requirements in Developing Them

During its assessment of allegation 2, the OIG determined PSF did not meet VA security requirements when developing the application programming interfaces. The team reviewed a judgmental sample of 35 VA security requirements from *The Department of Veterans Affairs Application Programming Interface Security Pattern*, issued June 25, 2018, and found that PSF Lighthouse application programming interfaces did not meet six of them in fiscal year 2019.[9] In two instances, PSF used alternative security protocols instead of what was required. However, the security pattern did not provide exemptions if alternative security protocols were used. Also, delays in publishing the security pattern led to some of the requirements not being promptly met. If these security deficiencies are not corrected, VA systems are at risk of unauthorized access, jeopardizing the confidentiality and integrity of VA and veteran data.

What the OIG Recommended

The OIG made two recommendations to the acting chief information officer regarding the applications without federal authorization. First, determine whether to prevent employees from using the SaaS applications named in the allegation that lack authority to operate. Second, determine whether federal authorization is required for one of the additional 19 applications reviewed and obtain authorization or report the issue to the Federal Chief Information Officer.

Regarding application programming interfaces, the OIG made two recommendations to the acting chief information officer to ensure that PSF improves security controls and documentation. First, either implement JavaScript Object Notation Web Encryption for Lighthouse application programming interfaces that transmit sensitive information and resource-sharing requirements for cross-origin resource sharing or seek exceptions to the standards. Second, implement alerts for application programming interface-related abuse to meet the standard.

Management Comments

The acting chief information officer concurred with the four recommendations and provided corrective action plans that are responsive to the recommendations. Appendix B includes the full text of the chief information officer's comments. The OIG will monitor implementation of the

[9] VA Office of Information Security, *The Department of Veterans Affairs Application Programming Interface Security Pattern*, ver. 1.2, June 25, 2018.

planned actions and will close the recommendations when OIT provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FedRAMP	Federal Risk and Authorization Management Program
FY	fiscal year
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	information technology
OIG	Office of Inspector General
OIS	Office of Information Security
OIT	Office of Information and Technology
OMB	Office of Management and Budget
PSF	Project Special Forces
SaaS	software as a service
URL	Uniform Resource Locator

Introduction

Cloud computing is a data management solution that allows VA—and other federal agencies and departments—ubiquitous, convenient, on-demand network access to information. As part of its day-to-day operations, VA must handle vast amounts of sensitive data, including veterans' healthcare information, through a number of cloud-based applications. This information needs to be accessed from various locations and by many employees, but with easy access comes potential security risks. If VA does not comply with federal security requirements for storing data in the cloud, then it could compromise veterans' protected and sensitive information.

In April 2019, the VA Office of Inspector General (OIG) received allegations that a division in VA's Office of Information and Technology (OIT) called Project Special Forces (PSF) was not following federal or VA policy for software-as-a-service (SaaS) applications.[10] SaaS applications are hosted and managed by a third-party software cloud service provider.

Federal and VA policies require that applications first have a Federal Risk and Authorization Management Program (FedRAMP) authorization before being allowed to operate on the VA network. PSF is the unit responsible for assisting with helping procure and implement SaaS applications.

The specific allegations made to the OIG pertained to some applications being unauthorized or managed outside established lines of authority:

1. **Unauthorized applications.** OIT allegedly allowed SaaS applications that were not FedRAMP authorized to be used on VA's network, and PSF allegedly advocated the use of nine unauthorized SaaS applications (Dropbox, Google Drive, iCloud, GitLab, SlideShare, Evernote, Basecamp, Datadog, and PagerDuty), putting VA and veterans' data at risk.
2. **Improperly managed applications.** PSF allegedly was also developing VA applications for the cloud that were managed outside the VA Enterprise Cloud group, which is responsible for all VA cloud assets. While evaluating the merit of this allegation, the OIG also assessed whether PSF developed and deployed application programming interfaces and services in compliance with VA security standards.

The OIG conducted this review to assess the specific allegations and, for allegation 1, examined the larger issue of whether OIT was fully following VA policy and FedRAMP authorization requirements for SaaS applications. While evaluating the merit of allegation 2 regarding PSF

[10] Office of Management and Budget (OMB), Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; VA Directive 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016.

developing cloud-based applications managed outside the VA Enterprise Cloud group, the review team also assessed whether the applications complied with VA security standards.

Cloud First Policy

Since 2010, the federal government has advocated that agencies embrace the cloud—a model for enabling abundant, convenient, on-demand network access to information that can be rapidly provisioned and released. The federal government's policy related to the cloud, known as Cloud First, requires agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. According to the White House's *25 Point Implementation Plan to Reform Federal Information Technology Management*, the benefits of moving to the cloud include reduced costs, greater flexibility, and eliminating long procurement and certification processes.[11]

FedRAMP

In December 2011, the Federal Chief Information Officer issued a memorandum introducing FedRAMP.[12] FedRAMP is a government-wide program that provides a standardized approach to security, authorization, and continuous monitoring for cloud products and services. Before FedRAMP, cloud service providers had to meet different security requirements for each federal agency. FedRAMP eliminates duplication by providing a common security framework, making it possible for agencies and cloud service providers to reuse authorizations. Agencies review a standardized set of security materials against one common baseline. A cloud service offering is authorized once, and the security package can be used by any federal agency. This saves money, time, and effort for both agencies and cloud service providers.

The memorandum established federal policy for protecting federal data in cloud services and defined executive branch responsibilities in developing, implementing, operating, and maintaining FedRAMP. Accordingly, VA is required to use FedRAMP when conducting risk assessments, granting security authorizations, and conferring an authority to operate when using cloud services, including SaaS applications.

In addition, the memorandum requires VA and other agencies to provide the Federal Chief Information Officer with a written certification every April 30 that lists all agency cloud services that cannot meet FedRAMP authorization requirements, along with an appropriate rationale and proposed resolutions.

FedRAMP is governed by different executive branch entities that collaborate to develop, manage, and operate the program. The Joint Authorization Board is the primary governance and

[11] Vivek Kundra, US Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010.

[12] OMB, Memorandum for Federal Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments."

decision-making body for FedRAMP and consists of the chief information officers from the Department of Defense, Department of Homeland Security, and General Services Administration. The Office of Management and Budget (OMB) is the governing body that issued the FedRAMP policy memorandum that defined key requirements and capabilities of the program. The Chief Information Officer Council disseminated FedRAMP information to federal chief information officers and other representatives through cross-agency communications and events. The National Institute for Standards and Technology advises FedRAMP on Federal Information Security Modernization Act compliance requirements.

SaaS Applications

SaaS products allow VA to use the service without having to maintain the system or manage the infrastructure. For example, VA uses DocuSign to send digital documents to patients for their signatures. VA can also use these SaaS applications to perform tasks such as automating code testing and executing workflows. A single cloud service provider often provides the same SaaS application to multiple government and nongovernment clients using shared infrastructure that it manages. SaaS applications are accessible from client devices through a web browser, which reduces maintenance costs because costs are split among all clients. These applications reside in cloud environments and allow for rapid expansion to many users.

SaaS Approval Process

OIT finalized an approval process for SaaS applications in April 2019. Under this process, when a business owner submits a request for a new SaaS application, PSF staff work with the business owner, the cloud service provider, and the Office of Information Security (OIS) to determine what information the SaaS application might contain and the potential risks associated with that information.[13] If all entities involved agree to proceed with the procurement, PSF staff work with the business owner and others in OIT to create the necessary acquisition documents, including providing the business owner with tailored language for procurement, such as requirements in the contract for the cloud service provider to obtain FedRAMP authorization, if still needed.

If the SaaS application has not received FedRAMP authorization, VA staff assist the cloud service provider through the FedRAMP authorization process. As part of this process, the cloud service provider is required to partner with an accredited third-party organization to complete a readiness assessment of its service offering. If the SaaS application has a FedRAMP authorization, VA can simply use the existing authorization.[14]

[13] The business owner is the entity that is requesting the service or application; the cloud service provider is a commercial or government agency providing cloud computing services.

[14] FedRAMP, *CSP Authorization Playbook: Getting Started with FedRAMP*, July 2018.

Along with the SaaS application obtaining FedRAMP authorization, multiple OIT offices, such as OIS, work to assess the application's security architecture and system risks, to highlight potential issues, and to provide mitigation recommendations. The Enterprise Program Management Office prepares a final risk review to present to an OIT authorizing official, who is responsible for making a risk-based decision on whether to grant the SaaS an authority to operate on VA's network. Figure 1 provides a high-level overview of the SaaS approval process.

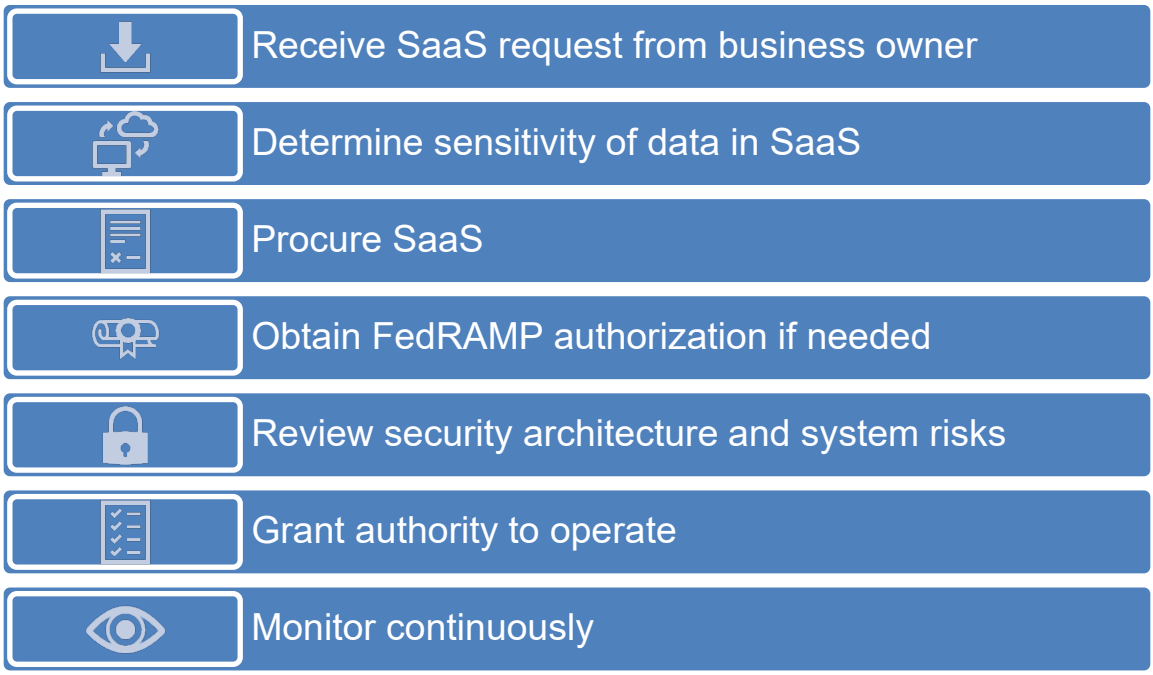

Figure 1. *VA OIT's SaaS approval process.*
Source: VA OIG analysis of information provided by OIT.

FedRAMP also allows federal agencies to sponsor a SaaS application through the authorization process. Using this approach, cloud service providers are still required to partner with a third-party assessment organization, but the authorizing official grants the SaaS application an authority to operate *before* FedRAMP authorization.[15] However, the OIG team determined that this approach was not used for any of the SaaS applications reviewed.

Lighthouse Application Programming Interfaces

OIT's Lighthouse is a platform that provides application programming interface developers with secure access to the VA data they need to create tools and services for veterans. Application programming interfaces are a set of routines, protocols, and tools for building software applications. The interfaces fall into five categories:

[15] FedRAMP, *CSP Authorization Playbook: Getting Started with FedRAMP*.

1. Benefits—allows organizations that assist veterans to digitally submit claim documents directly to the Veterans Benefits Administration's claims intake process and to request the status of a veteran's benefits claim on behalf of a veteran, and benefits interfaces allow the Veterans Benefits Administration to respond with the status of an appeal.
2. Health—helps veterans manage their health care, view their VA medical records, and share their information with caregivers and providers. Health interfaces also enable veterans to view their eligibility information to help them determine if they can receive urgent care or community care based on the veteran's proximity to a VA facility and its ability to provide the needed care.
3. Facilities—provides information about physical VA facilities including geographic location, address, phone number, hours of operation, and available services.
4. Forms—allows users to look up VA forms and check for new versions.
5. Veteran verification information—gives veterans control of their information by allowing them to choose who sees their information, including service history, veteran status, and discharge details.

Results and Recommendations

Finding 1: OIT Allowed Some Unauthorized Software to Be Used

The OIG substantiated the allegation that OIT was not fully following VA policy and FedRAMP authorization requirements for SaaS applications.[16] In addition to the nine applications that were included in the allegation about unauthorized use, the review team examined 19 other applications.

During testing, the OIG found that some of the nine SaaS applications alleged to be unauthorized were in use without FedRAMP authorizations. The OIG determined that VA had used eight of the nine SaaS applications, and of these eight, three still lacked the required FedRAMP authorizations. Also, as of March 9, 2020, seven of the eight SaaS applications used had not been authorized to operate on VA's network in accordance with policy. This lapse occurred because OIT allowed some external partners that did not meet VA security requirements to continue connecting to VA's network, decided to continue using legacy SaaS applications while they were going through the authority-to-operate process, and configured a SaaS application in a way that allowed it to penetrate the VA firewall without a risk assessment. However, the OIG did not substantiate that PSF advocated using any of the nine applications the complainant identified in the allegation.

The OIG determined that from June 2018 through March 9, 2020, OIT had approved 19 SaaS applications that PSF helped usher through the VA SaaS approval process for use on the network, but three of these applications lacked the required FedRAMP authorization, or were granted the authority to operate before obtaining the FedRAMP authorization.[17] This noncompliance occurred for two reasons: (1) OIT had not fully implemented a formal process for granting the authority to operate until April 2019; and (2) PSF staff misunderstood the FedRAMP authorization requirements for SaaS applications classified by OIT as low impact.[18]

By not meeting federal authorization requirements, VA is assuming unnecessary risks. Specifically, VA managers cannot ensure that the security controls to protect personally

[16] VA Directive 6517; VA Handbook 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016.

[17] VA Directive 6517. The directive requires that public SaaS applications have FedRAMP authorization before operating. According to OIT staff, PSF's assistance consisted of helping business owners complete procurement paperwork, providing acquisition language for service line agreements, and collaborating with the SaaS cloud service provider to complete FedRAMP documentation.

[18] National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," *Federal Information Processing Standard Publications (FIPS PUBS) 199*, February 1, 2004. These categorizations are based on the potential effect on an organization should the data be compromised.

identifiable information and protected health information contained in SaaS applications meet federal standards and will adequately protect veterans' data from unauthorized access.

This finding builds on the following observations:

- Some of the nine SaaS applications cited in the allegation lacked FedRAMP or VA authorization.
- Three of 19 SaaS applications examined during the review also lacked required FedRAMP authorizations.

What the OIG Did

Using the list of the nine SaaS applications named in the allegation, the review team obtained firewall traffic reports from OIT to determine which SaaS applications were being used by VA staff. The nine SaaS applications identified in the allegation were tested separately from the 19 approved SaaS applications referenced below. The team also researched the SaaS applications on the FedRAMP.gov marketplace to determine if FedRAMP had authorized them. In addition, the team conferred with multiple OIT divisions and reviewed the Enterprise Mission Assurance Support Service application, VA's information assurance program management application, to determine if VA had authorized the SaaS application.

The review team also asked OIT to provide a list of SaaS applications that were approved for use by VA as of March 9, 2020. For those 19 applications, the team reviewed the FedRAMP.gov marketplace and evaluated SaaS applications to determine whether FedRAMP authorizations were in place and when they were granted.[19] The review team later compared the date when the SaaS application was authorized by FedRAMP with the date VA granted the applications an authority to operate on VA's network.

In addition to reviewing guidance released by VA and OMB, the team reviewed documentation OIT provided to evaluate the merits of the allegations and to determine if there were broader concerns. The team conducted interviews with OIT and staff working for the FedRAMP program to gain an understanding of FedRAMP security requirements and the system authorization process. These interviews helped clarify the process OIT used to acquire and implement SaaS applications and PSF's role in the process.

Some of the Nine SaaS Applications Cited in the Allegation Lacked FedRAMP or VA Authorization

The allegation specified nine SaaS applications (Dropbox, Google Drive, iCloud, GitLab, SlideShare, Evernote, Basecamp, Datadog, and PagerDuty) that PSF allegedly advocated be used

[19] FedRAMP.gov marketplace is a dashboard that provides a searchable, sortable database of all cloud services that are FedRAMP authorized, FedRAMP ready, or in process for authorization.

throughout VA. Therefore, the review team looked at these nine applications separately. The team did not find evidence that PSF advocated for the use of the nine applications cited in the allegation. However, some of the nine SaaS applications that were allegedly not FedRAMP authorized were being used on the VA network. Most of these nine SaaS applications, listed in table 1, have cloud storage features available through the application's website. The team reviewed VA firewall traffic from April 1, 2019, through March 31, 2020, to determine whether VA staff were using them and determined that staff used eight of the nine. Of those eight, only one application, Google Drive, was authorized for limited use by VA staff and had FedRAMP authorization.

Table 1. SaaS Applications Cited in the Allegation, by Authorization Status

SaaS application	In use at VA	FedRAMP authorized	VA authorized
1. Basecamp	No	No	No
2. Datadog*	Yes	Yes	No
3. DropBox	Yes	No	No
4. Evernote‡	Yes	No	No
5. GitLab	Yes	No	No
6. Google Drive	Yes	Yes	Yes
7. iCloud	Yes	No	No
8. PagerDuty	Yes	No	No
9. SlideShare	Yes	No	No

Source: VA OIG analysis of SaaS usage on VA network.

**PSF is currently assisting Datadog and PagerDuty applications through the SaaS process.*

For DropBox, GitLab, and SlideShare, VA staff used an external partner network with a security setting not compliant with VA's standards. Work was completed to remedy this issue on January 5, 2021.

‡Evernote and iCloud were configured in a way that allowed them to pass through VA's firewall, but there was no documentation of authorization. However, in June 2021, VA configured Evernote filtering to impose some restrictions, and iCloud was configured to be used only for nonfederal data that did not require authorization.

OIT staff told the review team that PSF only assisted in the acquisition of two of the applications listed: Datadog and PagerDuty. Datadog is a data analytics application used to monitor databases, tools, and servers. PagerDuty helps customers prevent and resolve incidents that affect their business. For example, PagerDuty can notify customers in the event of a security breach. Because these two SaaS applications did not have authority to operate as of March 2020, the applications were not included on the list of VA-approved SaaS applications provided to the review team by OIT. Both SaaS applications were identified as being in use at VA before OIT

standardized the approval process. OIT assessed the applications, determined they were low risk, and decided to continue using them while they went through the SaaS approval process. OIT was working with Datadog as it went through the FedRAMP authorization process. OIT staff began but could not complete the approval process for PagerDuty because the cloud service provider was unwilling to go through the FedRAMP authorization process; OIT staff nonetheless allowed the application to remain on the network.

Two SaaS applications (Evernote and iCloud) were configured in a way that allowed them to pass through the VA's firewall, but OIT was unable to provide documentation to show that the applications had been granted authority to operate. The review team contacted multiple OIT divisions to determine why Evernote was allowed to pass through VA's firewall. OIT staff told the team that the application was configured to allow it to operate on the VA network, but they were unable to provide evidence that the SaaS had been approved to operate. Access to Evernote was partially restricted through OIT's use of Uniform Resource Locator filtering.[20] As of June 2021, Evernote was reconfigured to prevent it from passing through VA's firewall.

OIT staff said iCloud was allowed for personal use on government-issued electronic devices but that security settings were configured to prevent federal data from being collected or stored on the application. Since these additional security settings restricted iCloud use to accessing only nonfederal data, the application did not require FedRAMP authorization or a VA authority to operate.

Three SaaS applications—Dropbox, Gitlab, and SlideShare—were accessible by VA staff who were using an external partner extranet with a security setting below VA's standards, such as not requiring application or Uniform Resource Locator filtering.[21] This was initially done to avoid delays that filtering caused. OIT staff said they had been working for a while to bring the extranets up to VA's standards, but the process had been slow to ensure staff do not lose the use of applications that are mission critical. Work was completed on January 5, 2021.

Three of 19 SaaS Applications Lacked Required FedRAMP Authorizations

For the 19 SaaS applications examined during the OIG review, PSF assisted VA personnel and cloud service providers with navigating the SaaS approval process for using a desired application on the VA network. The review team found 14 were appropriately authorized by the proper VA official or did not require authorization. Three applications, however, did not have required

[20] Uniform Resource Locator (URL) is a short string containing an address that refers to an object on the web. URL filtering is when the firewall allows or denies Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) connections to a website based on an administrative policy of allowed and denied URL categories.

[21] An extranet is a connection that allows VA's external partners, such as contractors, access to VA's network.

FedRAMP authorizations when they were allowed to operate on VA's network, as shown in the bottom row of table 2.

Table 2. The 19 SaaS Applications Deployed to the Cloud during the Review Period by Status on Meeting Authorization Requirement

FedRAMP authorization status	Explanation	Example	Number of SaaS applications
Appropriately authorized	FedRAMP was authorized before responsible VA official granted authority to operate on its network.	FedRAMP authorized GitHub in October 2018, and a VA responsible official granted the SaaS the authority to operate on VA's network in February 2019.	3
Exempt because applications were internally developed on a FedRAMP-authorized platform to be used exclusively by VA	According to FedRAMP staff, applications developed and managed by VA on a FedRAMP-authorized platform do not require independent authorization.	HR Recruitment Activity Tracker is a SaaS application that was developed by VA on Salesforce, a FedRAMP-authorized platform. The SaaS was created, owned, and maintained by VA in a way that allows it to operate under the Salesforce FedRAMP authorization.	5
Exempt because they contained no VA-owned data	According to FedRAMP staff, a FedRAMP authorization is not required if the SaaS does not contain federal data.[22]	OIT staff reviewed Global Telehealth Services and found that the SaaS does not collect, process, or retain sensitive information.	8
Not appropriately authorized: VA approved the use before obtaining FedRAMP authorization	The responsible official approved use of a SaaS before FedRAMP authorization or personnel failed to obtain the authority to operate.	A VA authorizing official granted QGenda authority to operate in May 2019, but FedRAMP did not authorize QGenda until March 2020.	3

Source: VA OIG analysis of SaaS FedRAMP authorizations.

[22] OMB Circular A-130, "Managing Information as a Strategic Resource." OMB Circular A-130 defines federal information as "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form." According to OIS, VA uses the same definition to identify VA data.

The three applications that received VA's approval to operate before receiving a FedRAMP authorization were

1. IRBManager, which helps facilities meet Institutional Review Board requirements for biomedical research that will advance veterans' health care;
2. QGenda, which is used to schedule operating room staff; and
3. ServiceNow, which is a tool used for information technology (IT) service management, including handling help request tickets and resolving problems in various systems within VA that process employees' and veterans' identifiable information.

Two Applications Ultimately Received Authorization

OIT staff told the review team that two of the five SaaS applications—QGenda and ServiceNow—received authority to operate before FedRAMP authorization because OIT's process for acquisition and implementation of SaaS applications was new and informal. OIT staff put SaaS applications through the authority-to-operate and FedRAMP processes concurrently and ultimately granted authority for these applications to operate on VA's network before FedRAMP authorization, violating VA Directive and Handbook 6517.

Before granting the authority to operate for these two SaaS applications, OIT staff said they worked closely with the cloud service provider to perform security assessments equivalent to the reviews conducted by FedRAMP to ensure controls were appropriate.[23] In April 2019, OIT staff put a process in place for acquiring and implementing SaaS applications that follows FedRAMP security requirements. After April 2019, when the new intake process took effect, the OIG did not find instances of VA improperly granting an authority to operate before FedRAMP authorization. Because the new intake process addresses the security issues identified in the initial allegations to the OIG, no recommendations are offered regarding when VA grants the authority to operate.

One Application Still Lacked Authorization, Potentially Jeopardizing Veterans' Data

One application—IRBManager—was still not FedRAMP authorized as of July 2021, and staff said they had no plans to seek authorization for the application, as detailed below.[24] Staff explained that IRBManager was one of the first SaaS applications on which PSF assisted the cloud service business owner through the acquisition and approval process. OIT staff said that

[23] The review team did not assess the sufficiency of the OIT review or whether it was comparable to reviews performed during the FedRAMP authorization process.

[24] VA Directive 6517 requires SaaS applications to have FedRAMP authorization before deployment.

during this time, they misunderstood FedRAMP requirements for SaaS applications containing VA information categorized as low impact. In this case, they did not think a formal FedRAMP authorization was required. By March 2020, the misunderstanding was resolved, and OIT had issued a new flow chart for granting a VA authority to operate—one that clearly makes FedRAMP authorization a prerequisite for all SaaS applications.

Despite the clarification of low-impact SaaS requirements, OIT staff did not plan to obtain FedRAMP authorization for IRBManager because the cost involved in complying with FedRAMP would be prohibitive for the cloud service provider, a small business. Although the cloud service provider's situation is a practical consideration, it alone does not justify failing to comply with federal security requirements. In addition, OMB's *Security Authorization of Information Systems in Cloud Computing Environments*, effective December 8, 2011, requires agencies to provide the Federal Chief Information Officer written certification every April 30 that lists all agency cloud services that cannot meet FedRAMP authorization requirements, along with the rationale for accepting the associated risk and proposed mitigation measures. OIT personnel were unable to supply the review team any evidence that they had submitted this certification to the Federal Chief Information Officer.

Beyond compliance, the security of sensitive VA data in public SaaS applications is a concern. For example, IRBManager contains information needed to track safety and research studies, including VA employees' names, phone numbers, and work and personal email addresses. In addition, it includes volunteers' names and email addresses. According to the business owner for IRBManager, the SaaS application is not intended to track veterans' protected health information. However, the application includes free-text fields, which present the risk of protected health information and other personally identifiable information being manually entered into the application. Although OIT officials stated that a user could enter sensitive patient information, they explained that the system does not prompt staff to enter such data, and all content entered into the system is reviewed by multiple people with the ability to remove information that should not be there. OIT also stated that this risk has been mitigated through training, language in the system to discourage entering identifying information, and follow-up questions asking users whether identifying information was entered. Even though VA has taken steps to reduce the risks, allowing SaaS applications to operate on VA's network without FedRAMP authorization puts employee, volunteer, and veteran data at unnecessary risk of being improperly accessed.

Finding 1 Conclusion

For the nine SaaS applications identified in the allegation, the OIG did not find evidence that PSF advocated for the use of any of the SaaS applications. However, the OIG determined that eight of the nine SaaS applications were used by VA staff despite six of the eight not having FedRAMP required authorizations and seven of the eight not having authority to operate on the VA network. OIT has taken action to restrict access to some of these SaaS applications, but

two of the applications (PagerDuty and Datadog) still need to be assessed and either restricted from use or brought into compliance with VA and FedRAMP policy requirements. Accordingly, recommendation 1 addresses the risk of VA staff using unauthorized SaaS applications, which could expose sensitive data to misuse.

During its review, the OIG determined that one SaaS application (IRBManager) did not have the required FedRAMP authorization. Therefore, recommendation 2 addresses the need for FedRAMP authorization or submission of an appropriate certification to the Federal Chief Information Officer for VA to use IRBManager.

Veterans and employees should have confidence that their sensitive personal information is handled strictly in accordance with federal laws and VA policy. Not following FedRAMP authorization requirements and OIT policy can put sensitive data collected, processed, and retained by a SaaS application at risk of unauthorized access, modification, and destruction. By ensuring that SaaS applications have gone through the FedRAMP authorization process, adhering to the established definition of federal data, and reviewing the SaaS applications named in the allegation that did not have required FedRAMP or VA authorizations, VA can have assurance that VA staff use only approved and secure applications.

Recommendations 1–2

The OIG recommended that the acting chief information officer ensure the system owner take the following actions:

1. Review the SaaS applications named in the allegation to determine whether VA staff are still using them and whether such use is consistent with VA policy. If use is authorized, implement controls to ensure the applications go through the Federal Risk and Authorization Management Program authorization process and the VA SaaS application approval process. If use is not authorized, implement controls to prevent employees from using the SaaS applications without authority to operate.
2. Determine whether Federal Risk and Authorization Management Program authorization will be pursued for the IRBManager application. If the required federal authorization is not pursued, include this application in the annual certification letter to the Federal Chief Information Officer along with the appropriate rationale and proposed mitigation plan.

Management Comments

The acting chief information officer concurred with recommendations 1 and 2. To address recommendation 1, OIT will draft a clarifying memo for the use and security of SaaS applications. For SaaS applications named in the allegation, OIT will require application owners to identify those still in use and attest that those applications comply with VA policy. In addition,

PSF will work with OIT firewall team to determine if unauthorized systems are still in use and implement controls to prevent employees from using the SaaS applications without the authority to operate. The target implementation of these actions is within 180 days from October 7, 2021.

To address recommendation 2, OIT stated that IRBManager will be decommissioned in December 2021 and replaced with IRB NET system, which will soon be FedRAMP authorized.

OIG Response

The acting chief information officer's comments are responsive to the recommendations. The OIG will monitor the implementation of the planned actions and will close these recommendations when the OIG receives sufficient evidence demonstrating progress in addressing the issues identified.

Finding 2: The Correct Group Managed Application Programming Interfaces, but PSF Did Not Meet VA Security Requirements in Developing Them

Application programming interfaces allow third parties to "plug into" VA to send and retrieve data. The application programming interface capability simplifies and streamlines veteran access to VA data and services while reducing administrative burden. The OIG did not substantiate the allegation that PSF developed cloud-based applications that were managed outside the VA Enterprise Cloud group. The OIG determined that PSF's application development was limited to five Lighthouse application programming interfaces, which were hosted on the VA Enterprise Cloud and supported by the Enterprise Cloud Solutions Office (which oversees all VA cloud assets), consistent with established lines of authority. However, the OIG found OIT did not meet six of 35 selected VA security requirements when developing these application programming interfaces. When the review team asked PSF officials why they did not follow these requirements, they provided several reasons, including that OIS did not publish requirements on the VA Information Security Knowledge Service SharePoint site until March 2020 and that PSF used alternative security protocols.[25] However, the requirements did not give exemptions for using alternative security protocols. If the security deficiencies identified in this report are not corrected, VA systems increase the risk of unauthorized access that could endanger VA and veterans' data.

This finding builds on the following observations:

- The correct lines of authority were engaged in developing and managing OIT's PSF cloud interfaces.
- PSF did not meet some of VA's internal security requirements in developing application programming interfaces and in one instance employed an alternative protocol.

What the OIG Did

The OIG assessed the allegation that PSF-developed VA applications were being managed outside of the VA Enterprise Cloud group, which is responsible for the use of all VA cloud assets. The review team interviewed PSF personnel to identify PSF-developed applications and determine whether all applications were managed in accordance with VA and OIT policy. Interviewees included staff from PSF and the Demand Management Division of OIT's Enterprise

[25] The VA Information Security Knowledge Service SharePoint site is "VA's official site for enterprise Risk Management Framework policy and implementation guides. The OIS Knowledge Service provides cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forms, and the latest information and developments in the Risk Management Framework."

Program Management Office to clarify which parties were involved in developing the application programming interfaces.

OIG personnel reviewed the organizational structure of the Enterprise Program Management Office. The team also reviewed federal, VA, and OIT policy and guidance related to information security requirements for application programming interfaces. They examined information security requirements for systems under which PSF application programming interfaces were developed and through which external and internal VA users accessed them. Relevant personnel were interviewed to determine the source of VA application programming interface information security policy and guidance, and whether it applied to development of application programming interfaces in fiscal year (FY) 2019. Finally, the team selected a sample of VA application programming interface information security requirements to determine whether PSF implemented them in FY 2019.

The Correct Lines of Authority Were Engaged in Developing and Managing PSF Cloud Interfaces

The allegation stated that PSF-developed VA applications were being managed outside the VA Enterprise Cloud group, contrary to OIT's governing authority for managing cloud assets. VA's Enterprise Cloud hosts the department's web-based applications and is managed by the Enterprise Cloud Solutions Office. This office is the governing authority for utilization of all VA cloud assets.[26] The OIG determined that PSF's application development was limited to five Lighthouse application programming interfaces, which were hosted on the VA Enterprise Cloud and supported by the Enterprise Cloud Solutions Office, consistent with established lines of authority. As a result, the OIG did not substantiate the allegation that PSF developed software applications that were managed outside the VA Enterprise Cloud group.

PSF Did Not Meet Some Internal Security Requirements in Developing Application Programming Interfaces

In evaluating the allegations, the review team assessed broader compliance with VA security standards. OIS established security requirements for VA application programming interfaces in *The Department of Veterans Affairs Application Programming Interface Security Pattern*, effective June 2018.[27] The security pattern defines standards and guidelines for these interfaces employed by VA, explains discovery of them, and emphasizes ensuring interoperability and making data available to users and developers. The scope includes application programming

[26] VA memorandum, "Use of Software-as-a-Service (SaaS), Managed Services, and Cloud-Based Native Technologies and Approaches," April 10, 2018.

[27] VA OIS, *The Department of Veteran Affairs (VA) Application Programming Interface Security Pattern*, ver. 1.2, June 25, 2018.

interfaces developed internally by VA, as well as those provided by external entities and used by VA to achieve business objectives.

The security pattern was developed in coordination with the Application Programming Interface Strategy and Policy Working Group, which included representatives from the chief information officer's office, VA Digital Service, Privacy Office, Enterprise Architecture, Cybersecurity Operations Center, Enterprise Cloud Solutions Office, and Solutions Delivery. Several officials from OIS said that they developed these requirements because VA did not have any policies addressing the security needs of their application programming interfaces.

The review team discovered that the final version of the OIS Security Pattern, dated June 2018, was not published to the VA Information Security Knowledge Service's SharePoint until March 2020 due to an OIS staff mistake. Due to the delays in publishing the security pattern document, PSF staff believed the requirements were not applicable in FY 2019. However, OIS staff provided all stakeholders with a copy of the security requirements in 2018, along with the stated expectation that PSF would develop application programming interfaces following the security pattern requirements. In addition, PSF staff agreed that the security pattern includes important application programming interface design and security practices. Therefore, the OIG proceeded with identifying instances of noncompliance with the requirements detailed in this security pattern and provided recommendations for corrective action to ensure the security of VA application programming interfaces.

With the assistance of an OIG IT specialist, the team reviewed a judgmental sample of 35 requirements, focusing on those the team believed are most important for developing, releasing, and managing application programming interfaces. The team found that PSF Lighthouse application programming interfaces did not meet six of the 35 requirements reviewed for FY 2019. PSF took actions during FY 2019 and FY 2020 to satisfy some of the requirements. However, corrective actions are still needed to meet VA security requirements for web encryption, alerts for application programming interface-related abuse, cross-origin resource-sharing implementation (two requirements), consolidation of application programming interface documentation, and appropriate publication of Lighthouse application programming interfaces, as discussed in the sections that follow.

Transport Layer Security Was Used to Encrypt Application Programming Interfaces instead of JavaScript Object Notation Web Encryption

PSF did not implement JavaScript Object Notation Web Encryption, although VA standards require it for transmitting sensitive information and allow no exemptions.[28] PSF staff said they do not use this method of encryption because they use other methods they believe are equally secure. Specifically, they use Transport Layer Security for end-to-end encryption and OAuth for authentication of application programming interface users. According to PSF staff, JavaScript Object Notation Web Encryption is not required where Transport Layer Security and OAuth are both used. PSF staff also said using both JavaScript Object Notation Web Encryption and the combination of Transport Layer Security and OAuth would be counterproductive. PSF staff said they would pursue a change to VA standards to allow for the use of either JavaScript Object Notation Web Encryption or the combination of Transport Layer Security encryption and OAuth authorization controls. As of June 2021, PSF had not implemented the JavaScript Object Notation Web Encryption but planned to work with OIS to have the requirements changed.

Certain Resource-Sharing Controls Did Not Align with Requirements

PSF did not meet two requirements related to cross-origin (origin meaning domain, scheme, or port) resource sharing for the Lighthouse application programming interfaces in FY 2019.[29] The requirements were to (1) disable cross-origin resource-sharing methods that are not supported or required, and if these methods are not disabled, (2) prohibit the use of wildcards (symbols such as *) to represent unspecified characters in code identifying the requester and the preferred resource-sharing method.

A PSF contractor stated that cross-origin resource sharing is required and consequently was not disabled. Additionally, despite security pattern requirements, PSF staff implemented controls that use wildcards. The PSF contractor further stated that while the use of wildcards through the gateway does not meet security pattern requirements, access to their application programming interfaces was secure because PSF uses path-based routing of internet requests to different locations based on the originating web address. PSF staff also maintained that their use of

[28] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 5.2.2. The guidance states, "Developers shall implement Representational State Transfer application programming interfaces in accordance with Request for Comments (RFC) 7516 JavaScript Object Notation Web Encryption for protected health information, Payment Card Industry, and personally identifiable information." Internet Engineering Task Force RFC 7516 defines JavaScript Object Notation Web Encryption as a specification that standardizes the way to represent encrypted content in a JavaScript Object Notation-based data structure.

[29] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 5.3.1. Note that cross-origin resource sharing allows the browser and server to communicate about which internet-based requests are allowed.

cross-origin resource sharing meets the intent of the security pattern requirements. They planned to work with OIS to accommodate their gateway use cases.

Improper implementation of cross-origin resource sharing could result in the failure to validate or approve requesters seeking to use VA application programming interfaces and lead to unauthorized access to VA and veteran data.

Alerts for Application Programming Interface-Related Abuse Were Not Implemented

Lighthouse application programming interfaces did not implement alerts for interface-related abuse—e.g., denial of service or authentication attempts—in FY 2019 as required.[30] Alerts notify designated personnel of actual or potential compromises to information systems. When alerts are not in place, systems may be subject to unauthorized access without the knowledge of system owners. As of June 2021, PSF had not implemented alerts for application programming interface-related abuse, but PSF officials stated they were working on doing so.

Developer-Focused Application Programming Interface Documentation Was Not Consolidated

PSF staff did not create and maintain developer-focused documentation of application programming interfaces in the form of a standard operating procedure or a guide, as required.[31] OIS's Enterprise Security Architecture staff said developers of external application programming interfaces need easy access to Lighthouse application programming interface procedures and processes so that they can be aware of and comply with VA requirements. They further stated the intent of this requirement was to have this guidance consolidated in one location. PSF staff created and maintained developer-focused application programming interface documentation but stored it in various Lighthouse web pages and repositories. PSF staff explained the documentation was created by different teams over time and not consolidated. A PSF manager acknowledged the need for developers to understand PSF processes and said the unit plans to locate the documents centrally. As of June 16, 2021, PSF had consolidated the documents on the VA Lighthouse application programming interface website. Consolidating developer-focused documentation gives new developers the required information and tools to develop external application programming interfaces in compliance with VA and Lighthouse application programming interface requirements. Therefore, no recommendations are offered.

[30] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 5.2.3; VA Handbook 6500, app. F, SI-4(5), *Information System Monitoring (P1), System-Generated Alerts*, March 10, 2015.

[31] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 4. The guidance states, "Application programming interface Providers shall create and maintain developer-focused application programming interface documentation (e.g., Standard Operating Procedures and Privileged Users Guides)."

Lighthouse Application Programming Interfaces Were Not Published to Appropriate VA Sites

Although PSF Lighthouse application programming interfaces are required to be included in the VA Enterprise Architecture Repository, the interfaces were not included there.[32] This repository hosts data and organizes basic information about them to facilitate discovery and exchange of information across VA. In addition, PSF's Open Data application programming interface was not published on VA's Open Data Portal as required.[33] PSF staff said they were not aware of the requirements due to the delayed publication of guidance (the security pattern) on the VA Information Security Knowledge Service SharePoint site. In addition, they said their application programming interfaces are located on the Lighthouse application programming interface website (https://developer.va.gov), which is publicly available, but does not meet the security pattern requirement. On January 22, 2021, PSF published its Open Data application programming interface on the VA's Open Data Portal, and as of June 16, 2021, PSF had included Lighthouse application programming interfaces in the VA Enterprise Architecture Repository. Accordingly, no related recommendations are offered.

Finding 2 Conclusion

VA's Application Programming Interface Security Pattern establishes security requirements to assist VA as it adopts cloud technologies and more modern applications and system architectures. The security pattern states, "Application programming interfaces have unique security considerations, including the fact that they are often designed to access larger amounts and types of data, may have the potential to access backend servers or databases, and have different usage patterns."

In developing application programming interfaces, PSF did not meet security requirements defined in the security pattern. Information passing through Lighthouse application programming interfaces or other VA systems were put at risk of unauthorized access or for mishandling of sensitive veteran data or information. Recommendation 3 is for OIT to implement JavaScript Object Notation Web Encryption for Lighthouse application programming interfaces that transmit sensitive information so that they meet requirements for cross-origin resource sharing. Alternatively, OIT should coordinate with OIS to determine if modifications or exceptions to standards are warranted.

---

[32] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 4. The guidance states that "VA's authoritative repository for application programming interface shall be the VA Enterprise Architecture Repository."

[33] VA OIS, *VA Application Programming Interface Security Pattern*, sec. 3.1. The guidance defines Open Data application programming interfaces as "public-facing resource endpoints that can be consumed by the developer community at large, inside as well as outside an organization. VA's Open Data application programming interfaces are made available via the VA Open Data portal (https://www.data.va.gov)."

OIT did not ensure that certain security control and documentation requirements were met when developing application programming interfaces. Specifically, cross-origin resource sharing for application programming interfaces was not implemented; maintaining a centralized location for application programming interfaces was not developed; and VA's Enterprise Architecture Repository did not include information on application programming interfaces. In view of these deficiencies, recommendation 4 is for OIT to meet requirements by implementing alerts for application programming interface-related abuse. These requirements are meant to protect VA from unauthorized access that can put veteran information and other sensitive or protected information at risk. Although the review team did not learn of any incursions or mishandling of data, the OIG has offered recommendations to help VA focus on ensuring its own guidance is followed and to evaluate all alternatives used in the interim to inform any additional revisions to policies and practices. Until OIT implements the recommended corrective actions, veterans will not have confidence that their sensitive information is effectively safeguarded.

Recommendations 3–4

The OIG recommended that the acting chief information officer ensure Project Special Forces leaders take the following actions:

3. Implement JavaScript Object Notation Web Encryption for Lighthouse application programming interfaces that transmit sensitive information and resource-sharing requirements for cross-origin resource sharing to meet the requirements of VA Office of Information Security's Application Programming Interface Security Pattern. Alternatively, coordinate with the Office of Information Security to determine if modifications or exceptions to security standards are warranted.
4. Implement alerts for application programming interface-related abuse to meet the requirements of the VA Office of Information Security's Application Programming Interface Security Pattern.

Management Comments

The acting chief information officer concurred with recommendations 3 and 4. To address recommendation 3, OIT will "extend the security patterns to allow for Transport Layer Security and OAUTH in lieu of JavaScript Object Notation Web Encryption when securing Application Programming Interfaces exchanging personal health information." In addition, OIT will "extend the security pattern to allow for exceptions to cross-origin resource sharing requirements" as need dictates. The target implementation date for these actions is within 90 days from the October 7, 2021, transmittal memo with OIT comments on the report recommendations.

For recommendation 4, OIT reported it "has implemented all the monitoring and detection of application programming interface abuse events as specified in the security pattern and is sending alerts to a test channel. The last remaining work is to change the alerting to a production

channel. The Office of Information Security and PSF will also incorporate protocols within standard operating procedures to address this concern." OIT stated that it planned to implement these actions within 90 calendar days from October 7, 2021, as well.

OIG Response

The acting chief information officer's comments are responsive to the recommendations. The OIG will monitor the implementation of the planned actions and will close these recommendations when the OIG receives sufficient evidence demonstrating progress in addressing the issues identified.

Appendix A: Scope and Methodology

Scope

The OIG conducted this review to assess the allegations that OIT was not fully following VA policy and FedRAMP authorization requirements for SaaS applications. The OIG also evaluated the allegation that PSF developed cloud-based applications that were managed outside the VA Enterprise Cloud group. The review team conducted its work from November 2019 through August 2021.

Methodology

To accomplish its objective, the review team identified and reviewed applicable laws, regulations, and VA policies and procedures related to FedRAMP authorization and computer security during development of application programming interfaces.

The team interviewed OIT staff to obtain information related to SaaS applications. To assess PSF's compliance with FedRAMP authorization requirements, the team reviewed a list of 19 SaaS applications provided by PSF staff. To determine whether authorizations were granted in accordance with policy, the team reviewed public information on the FedRAMP Marketplace website and documentation on VA's Enterprise Mission Assurance Support Service to determine when FedRAMP authorized the SaaS applications and when VA granted them an authority to operate on VA's network.[34]

For the first objective, the review team determined whether VA staff was using the SaaS applications cited in the allegation. Internal firewall traffic reports from OIT's IT Operations and Services Division indicated how many times a user was able to successfully access the SaaS from April 1, 2019, through March 30, 2020. The team interviewed OIT staff in the Enterprise Security External Change Council, Cybersecurity Operations Center, and Network Operations Center to determine whether the SaaS applications were approved for use without obtaining an authority to operate.

To address the second objective, the review team interviewed senior PSF staff and reviewed VA memorandums to determine whether PSF developed applications that were being managed outside the VA Enterprise Cloud group. The team reviewed OIT organization charts, internal documents, and information contained in VA's Enterprise Mission Assurance Support Service to

[34] The Enterprise Mission Assurance Support Service is a cybersecurity governance, risk, and compliance tool designed to allow federal agencies to track the authorization of systems and provide the status of the associated milestones.

determine whether the application programming interfaces were developed under the authority and support of the Enterprise Cloud Solutions Office.

The team interviewed staff from OIS to obtain information about VA OIS Enterprise Security Architecture and the development of VA standards related to application programming interfaces. To determine whether security controls were in place for PSF-developed application programming interfaces in FY 2019, the team reviewed information security documentation relating to information systems under which PSF applications were developed. This review included system security plans, risk management framework security assessment reports, and system vulnerability scans, as well as controls in place for external and internal access to the PSF applications. In addition, the team reviewed documentation related to the application programming interfaces on VA's internet and intranet web sites and the GitHub repository, where information for the development and management of the application programming interfaces are stored. Specifically, the review team examined security assessment reports, systems security plans, and system vulnerability scans performed by VA OIT staff. Finally, the team reviewed judgmental sample of information security controls developed for VA application programming interfaces to determine if the controls met VA requirements in FY 2019.

Data Reliability

The team evaluated the accuracy of the SaaS application list provided by PSF by comparing the data security category on the list to documentation the review team obtained from PSF's SharePoint site; Enterprise Mission Assurance Support Service; and from OIT staff. To review the accuracy of the data security category, the team reviewed privacy threshold assessments and data security categorizations for the listed SaaS applications. The team found that some of the data security categories for SaaS applications on PSF's application list did not match the documentation the team reviewed.

The team interviewed and discussed the discrepancies with PSF staff, who either agreed that the list provided was erroneous or could not explain the discrepancies. Based on the discrepancies found, the team concluded that the PSF application list was not accurate. The review to determine whether SaaS applications had the appropriate FedRAMP authorization only focused on applications that PSF assisted through the SaaS intake process. However, the OIG was unable to independently generate a list of approved SaaS applications that PSF facilitated, due to filtering limitations of OIT applications. Therefore, the team relied on PSF to identify which applications it assisted in approving. To mitigate the risk of inaccuracy, the review team required additional documentation to support statements made by PSF staff regarding SaaS applications. With that documentation, the review team concluded that the information obtained and used was sufficiently reliable for the purposes of this review.

Fraud Assessment

The review team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the review objectives, could occur during this review. The team exercised due diligence in staying alert to any fraud indicators by taking actions such as engaging the OIG's Office of Investigations and reviewing possibly relevant OIG hotline complaints and concerns. The OIG did not identify any instances of fraud or potential fraud during this review.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The evidence obtained provides a reasonable basis for the OIG's findings and conclusions based on the OIG's review objective.

Appendix B: Management Comments, Office of Information and Technology

Department of Veterans Affairs Memorandum

Date: October 07, 2021

From: Chief Officer, Connected Care, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: OIG Draft Report, VA Applications Lacked Federal Authorizations and Interfaces Did Not Meet Security Requirements (Project No. 2020-00426-CT-0001)

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, "VA Applications Lacked Federal Authorizations and Interfaces Did Not Meet Security Requirements." The Office of Information and Technology submits the attached written comments.

The OIG removed point of contact information prior to publication.

(Original signed by)

Neil C. Evans, M.D.

Attachment

005 Attachment

Department of Veterans Affairs (VA) Comments to Office of Inspector General (OIG) Report, VA Applications Lacked Federal Authorizations and Interfaces Did Not Meet Security Requirements, Project No. 2020-00426-CT-0001

OIG Recommendation 1: The OIG recommends the acting Chief Information Officer ensure the system owner review the SaaS applications named in the allegation to determine whether VA staff are still using them and whether such use is consistent with VA policy. If use is authorized, implement controls to ensure the applications go through the FedRAMP authorization process and the VA SaaS application approval process. If use is not authorized, implement controls to prevent employees from using the SaaS applications without authority to operate.

Comments: Concur. The Office of Information and Technology (OIT) will draft a clarifying memo for the use and security of Software as a Service (SaaS) applications. For SaaS applications named in the allegation, OIT will require application owners to identify those still in use and attest that those applications comply with Department of Veterans Affairs (VA) Policy. Digital Transformation Center (DTC)/Project Special Forces (PSF) will work with the OIT Firewall team to determine if unauthorized systems are still in use and implement controls to prevent employees from using the SaaS applications without the Authority to Operate (ATO). Target implementation date: actions will be completed within 180 calendar days.

Status: Implementation of this recommendation is still in progress.

OIG Recommendation 2: The OIG recommends the acting Chief Information Officer ensure the system owner determine whether Federal Risk and Authorization Management Program authorization will be pursued for the IRB Manager application. If the required federal authorization is not pursued, include them in the annual certification letter to the Federal Chief Information Officer along with the appropriate rationale and proposed mitigation plan.

Comments: Concur. The vendor for IRB Manager communicated that they do not wish to pursue Federal Risk and Authorization Management Program (FedRAMP) authorization due to cost effectiveness. In addition, the VA Business Customer does not have the funding to support the authorization of IRB Manager. (Note:IRB Manager contract was awarded by the VA Business Customer prior to DTC/PSF engagement). In June 2021, IRB Manager was granted an extension on its VA ATO by VA's Authorizing Official to allow migration to the IRB NET and is in the process of being decommissioned (December 2021) and replaced with the soon-to-be FedRAMP authorized IRB NET system. The target implementation date for decommissioning of IRB Manager is December 31, 2021.

Note: A security authorization decision was attached to the response.

Status: Implementation of this recommendation is still in progress.

OIG Recommendation 3: The OIG recommends the acting Chief Information Officer ensure Project Special Forces leaders implement JavaScript Object Notation Web Encryption for Lighthouse application programming interfaces that transmit sensitive information and resource sharing requirements for cross-origin resource sharing to meet the requirements of VA Office of Information Security's Application Programming Interface Security Pattern. Alternatively, coordinate with the Office of Information Security to determine if modifications or exceptions to security standards is warranted.

Comments: Concur. OIT will extend the security patterns to allow for Transport Layer Security and OAUTH in lieu of JavaScript Object Notation Web Encryption when securing Application Programming Interfaces exchanging personal health information. OIT will also extend the security patterns to allow for

exceptions to cross- origin resource sharing requirements as use case dictates. Target implementation date: actions will be completed within 90 calendar days.

Status: Implementation of this recommendation is still in progress.

OIG Recommendation 4: The OIG recommends the acting Chief Information Officer ensure Project Special Forces leaders implement alerts for application programming interface-related abuse to meet the requirements of the VA Office of Information Security's Application Programming Interface Security Pattern.

Comments: Concur. OIT has implemented all the monitoring and detection of application programming interface abuse events as specified in the security pattern and is sending alerts to a test channel. The last remaining work is to change the alerting to a production channel. The Office of Information Security and PSF will also incorporate protocols within standard operating procedures to address this concern. Target implementation date: action will be completed within 90 calendar days.

Status: Implementation of this recommendation is still in progress.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection/Audit/Review Team	Michael Bowman, Director John Cefai Barbara Ferris Javon Johnson Erin Routh
Other Contributors	Michael Soybel Allison Tarmann

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.va.gov/oig.