OSC File No. DI-22-000742

Comments specific to the original report:

[redacted], February 20, 2024

Page 8 states that, for cases that are incorrectly marked “non-sensitive” there are 2,010 VIEWS users that can download, screenshot, and share sensitive and Veterans data without a need to know, and without the knowledge of the business owners.

The page also states that all VIEWS users have access to some 3.6M Veterans records in the VIEWS CCM contacts database to include name, date of birth, personal addresses, and phone numbers.

Comment:

[redacted], February 20, 2024

I appreciate the Secretary’s sincerity in taking the allegations seriously. I also appreciate, however belatedly, the Department’s steps in creating a more secure VIEWS system.

I am very concerned that the revelation that Veterans’ and whistleblowers information is available to users without their knowledge or consent will erode trust in the agency; and second, that whistleblowers who now know their information can be seen by users without a need to know will be unwilling to come forward, fearing what will happen to their careers if they do. The Department will lose a lot of money and those who need to be held accountable will not be. This is why the Department must mitigate as much as possible, what has already happened here.

One of the ways the Department could help is by creating a training module that is specific to whistleblower and Veterans Information. For instance: Are all whistleblower and Veterans information supposed to be stored in VIEWS as a database? Why is it that some organizations, such as OSC do not upload into VIEWS, but other organizations, such as OAWP, upload cases into VIEWS? Surely there is duplicative effort going on here that doesn’t need to be. The employee’s allegations could be in a database at OAWP without going into VIEWS, or at OIG without going into VIEWS, as examples.

To take a hypothetical example, suppose Employee A makes an allegation against their boss, Supervisor B. They have been trained in VIEWS, have access to the system, and are in the same organizational mailbox. The whistleblower in good faith, made these allegations and went to an external organization, such as OAWP or OIG. What the whistleblower doesn’t know is that another employee opens up a case and stores the whistleblower’s OAWP or OIG case into VIEWS without their knowledge or consent. Even if the case is marked sensitive, the employees in the organizational mailbox could still see the employee’s allegations. Supervisor B, who is part of the organizational mailbox, could also see the allegations, and potentially take an adverse action against the employee.

Now let’s suppose that the whistleblower’s allegations are substantiated, and as part of the settlement, the whistleblower moved onto another team at VA. He or she is trying to move on with their lives, as the whistleblowing has taken an emotional toll on the employee. If the employee’s allegations from their previous office are available to the 2,010 VIEWS users at the time the report was created, chances are someone in the new organization searches the name, tells the new supervisor at the new organization, and the employee, who was trying to get over what happened to them, cannot.

We owe it to our employees, Veterans, their caregivers, survivors, and whistleblowers, to ensure that instances like this do not happen, and that VA is a world class organization.

I also suggest that the Department consider asking Salesforce to create a default function which allows an email or document to be encrypted if it does have to be stored in VIEWS. In this way, a general user could not access the document related to the whistle-blower case.

General comment #2, for both the supplemental report and original report:

[redacted], February 20, 2024

The Department states that holding people accountable will take many man hours and suggest that there are too many VIEWS cases, requiring VA leadership attention (I think the quote was 260 VIEWS cases per day) to reliably determine who is responsible.

As a general VIEWS user, I can share that finding responsible parties is not as difficult, and would not take as much time, as the Department thinks. When a case is opened, there is a timestamp; similarly; when a document is uploaded there is a timestamp, and a name attached. When a VIEWS user closes a case, they have to fill out close case details. Even if the employee was directed by someone else to open or close a VIEWS case with whistleblower or Veterans' information in it, the employee would certainly be able to tell an investigator who directed them to store that information in the system.

As an alternative, the Department could ask either Salesforce, who built VIEWS for the Department, to locate cases or accounts that are suspicious in VIEWS or have one of their team members reach out directly to the owner of the organizational mailbox. These steps would go along way to restoring confidence in the Department when storing Veterans' or whistleblower's sensitive information.

General comment #3, supplemental report:

The Department states that there was inadequate training on the part of the VIEWS users.

[redacted], February 20, 2024

Comment: I thought the training was adequate. I am sure when VIEWS was first built, the Department had certain requirements; but sometimes the requirements change and the system or training has to be updated. The Department should refresh their system training if they feel it was inadequate.