DISTRICT COURT OF THE VIRGIN ISLANDS
DIVISION OF ST. THOMAS AND ST. JOHN

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 3:08-cv-00158**
	)	
THE TERRITORY OF THE VIRGIN ISLANDS and the VIRGIN ISLANDS POLICE DEPARTMENT,	)	
	)	
Defendants.	)	

ORDER

BEFORE THE COURT is the motion of the Virgin Islands Police Department ("VIPD") requesting that the Court "enter an order permitting VIPD to enter into IAPro historical data dating back to July 2017 which were lost during the 2019 ransomware and virus attacks on VIPD's network." (ECF No. 471.)

In 2008, the United States of America filed this action against the Territory of the Virgin Islands and the VIPD pursuant to the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141.

In March 2009, the Court approved the Consent Decree in this matter. (ECF No. 3.) In the Consent Decree, the VIPD agreed to implement comprehensive reforms to ensure that the VIPD delivers constitutional, effective policing services that promote public safety and police integrity. The Consent Decree requires a complete review and update of VIPD's use of force policies, training, and practices, as well as the implementation of internal and external systems of accountability that will ensure the sustainability of critical reforms.

In particular, Consent Decree Paragraphs 59 through 68 require the implementation of a risk management system intended to promote civil rights and best police practices, manage risk and liability, and evaluate the performance of all VIPD officers through the storage and analysis of various data regarding uses of force and citizen complaints. Pursuant to Paragraph 65, the VIPD must maintain "all personally identifiable information about an officer included in the risk management system during the officer's employment with the

VIPD for at least five years." *See* Consent Decree at 15, ECF No. 3. Additionally, "[i]nformation necessary for aggregate statistical analysis will be maintained indefinitely in the risk management system." *Id.*

To meet the requirements of Consent Decree Paragraphs 59 through 68, the VIPD has been using IAPro, a risk management software package, since 2010. The VIPD also maintains hard-copy paper records of the data uploaded into IAPro.

Recently, VIPD lost electronic access to years of historical data stored in IAPro due to an April 2019 ransomware attack and July 2019 virus that infected the VIPD's computer network. Since that time, the VIPD has reinstalled IAPro and has been re-uploading the historical data that was lost, beginning with the most recent historical data. To date, the VIPD has uploaded all historical data from 2018 to the present and is currently working on re-entering data from 2017.

On September 23, 2020, the VIPD filed a motion requesting that the Court "enter an order permitting VIPD to enter into IAPro historical data dating back to July 2017 which were lost during the 2019 ransomware and virus attacks on VIPD's network." (ECF No. 471.) On October 5, 2020, the United States filed a response indicating that it does not oppose the VIPD's motion. (ECF No. 475.)

The Court construes the VIPD's request as a motion to modify the Consent Decree to temporarily excuse the VIPD from the five-year data retention requirement of Paragraph 65. Indeed, the VIPD argues that (1) "requiring VIPD to re-enter data prior to July 2017 into IAPro would be too time-intensive and burdensome," ECF No. 471 at 3; (2) "restoring an electronic database of historical records dating back to July of 2017, while simultaneously inputting new contemporaneous records, is sufficient to satisfy the intent of Paragraph 59 to 'promote civil rights and best police practices, to manage risk and liability and to evaluate the performance of VIPD officers across all ranks, units and shifts,'" *id.* at 3-4; (3) "the purpose and spirit behind Paragraph 65's requirement of maintaining personally identifiable information regarding each VIPD officer for at least a period of five years can still largely be achieved with a combination of electronic and paper records," *id.* at 4 (quotations marks omitted); and (4) the VIPD will still allow "to efficiently and adequately conduct data

analysis, identify patterns and trends and evaluate the activity of VIPD's personnel over a reasonable period of time," *id.*

In *Rufo v. Inmates of the Suffolk County Jail*, 502 U.S. 367 (1992), the Supreme Court formulated a two-step process to determine whether a consent decree in an institutional reform litigation case should be modified and the extent of any such modification. *See* 502 U.S. at 383. Under the *Rufo* approach, "a party seeking modification of a consent decree bears the burden of establishing that a significant change in circumstances warrants revision of the decree." *Id.* When attempting to show the requisite change in circumstances, however, the party seeking modification ordinarily cannot rely "upon events that actually were anticipated at the time it entered into a decree." *Id.* at 385. If the moving party can meet its initial burden, the court may modify the decree if the modification is "suitably tailored to the changed circumstance." *Id.* at 383. The modification "must not create or perpetuate a constitutional violation"; it "should not strive to rewrite a consent order so that it conforms to the constitutional floor"; and a court should not try to modify a consent order except to make those revisions that equity requires, given the change in circumstances. *Id.* at 391.

Here, the VIPD effectively seeks to modify Paragraph 65 of the Consent Decree to excuse the VIPD from the requirement to maintain any data dated prior to July 2017 in its electronic risk management system, IAPro. The Court is convinced that the cyberattacks experienced by the VIPD in April and July of 2019 constitute an unanticipated, significant change in circumstances relating to the Consent Decree's requirements for data retention in its electronic risk management system. Moreover, given that (1) the VIPD maintains hard copy records of historical data and continues to upload current data into the risk management system, and (2) the entry of historical data lost due to the 2019 cyberattacks is significantly time-consuming and costly, the Court is persuaded that modifying Paragraph 65 of the Consent Decree to excuse the VIPD from the requirement to maintain any data dated prior to July 2017 in its electronic risk management system is suitably, and equitably, tailored to the changed circumstances in this matter. Indeed, the modification requested by the VIPD, which the United States does not oppose, will excuse the VIPD from the original five-year data retention requirement specified in Paragraph 65 only temporarily—by

continuing to upload current data, the VIPD will have an electronic database containing at least five years of data by July 2022. The Court agrees with the parties that, in the interim, the retention of a combination of electronic and hard copy records satisfies the spirit and intent of the Consent Decree and will still allow the VIPD to utilize its risk management system in a manner that promotes civil rights and best police practices, manages risk and liability, and evaluates the performance of all VIPD officers.

The premises considered, it is hereby

ORDERED that the motion of the VIPD, ECF No. 471, is **GRANTED**; and it is further

ORDERED that Paragraph 65 of the Consent Decree is **MODIFIED** to contain the following language at the end of that paragraph:

> Notwithstanding the foregoing, the VIPD shall not be required to upload any data dated prior to July 2017 into its electronic risk management system. Such data shall continue to be retained in hard copy form consistent with the foregoing requirements of this paragraph.

Date: October 29, 2020

/s/ Robert A. Molloy
ROBERT A. MOLLOY
District Judge