Before the Presiding Judges of the Administrative Judicial Regions
Per Curiam Rule 12 Decision

APPEAL NO.: 16-018

RESPONDENT: Judge David Crain, 331st Criminal District Court

DATE: March 8, 2017

SPECIAL COMMITTEE: Judge Steve Ables, Chairman; Judge David Peeples; Judge Missy Medary; Judge Dean Rucker; Judge David L. Evans

Petitioner requested from Respondent "any and all documents which reflect the time that Judge David Crain left the Blackwell-Thurman Criminal Justice Center on September 2, 2014 or which reflect that he was in the building until 5:00 p.m., including but not limited to calendar entries, computer usage records, computer log-in and log-out records, e-mails opened or sent, phone calls received or made, security pass data for the judge's garage door and security pass data for the judge's elevator door." Respondent informed Petitioner that no calendar entries existed and denied the request for the other information. Petitioner then filed this appeal. Respondent replied to the petition but did not provide any records for this committee's review.

Respondent asserts the information is exempt from disclosure under Rule 12.5(b) and Rule 12.5(i). Rule 12.5(b) exempts "any record, including a security plan or code, the release of which would jeopardize the security of an individual against physical injury or jeopardize information or property against theft, tampering, improper use, illegal disclosure, trespass, unauthorized access, or physical injury." Rule 12.5(i), exempts information that is confidential under a "state or federal constitutional provision, statute, or common-law." Respondent asserts that the responsive information is made confidential by Government Code Sec. 418.182(a), a provision of the Texas Homeland Security Act. This section reads: "Except as provided by Subsections (b) and (c), information, including access codes and passwords, in the possession of a governmental entity that relates to the specifications, operating procedures, or location of a security system used to protect public or private property from an act of terrorism or related criminal activity is confidential."

Garage door and elevator security pass data[1]

We first address whether security pass data for Respondent's garage door and elevator is exempt from disclosure under Rule 12.5(b) and (i). Respondent argues that the release of this data would jeopardize Respondent's security against physical injury and should be withheld based on

[1] We note that garage door and elevator security pass data is usually created and maintained by the Sheriff's Office or other entity responsible for courthouse security, not by the judiciary. However, because Respondent indicates that this data is in Respondent's possession and therefore, arguably, it is being maintained by the judiciary, we will address the exemptions Respondent has raised.

security concerns. Petitioner cited several Office of the Attorney General (OAG) letter rulings interpreting a comparable Public Information Act provision in support of his argument. Though we agree that the collection of security pass access data over a time-period may be used to determine a pattern of a person's comings and goings and consequently pose a security risk, we are not convinced that the release of this information for a one-day period indicating whether a person is in the building at a specific time would enable this type of observation or jeopardize Respondent's security against physical injury. The OAG letter rulings cited by Respondent do not persuade us otherwise. All of the cited letter rulings appear to involve requests for records spanning more than a day where patterns could be detected. Because the requested record is limited to one day, if such a record exists and is in the possession of Respondent, we conclude that it is not exempt from disclosure under Rule 12.5(b). We note, however, that this conclusion should not be interpreted to mean that garage and elevator security pass records are never exempt under Rule 12.5(b). Our conclusion is limited to the facts of this appeal.

Respondent also maintains that these records are confidential under Sec. 418.182(a) of the Government Code and are therefore exempt under Rule 12.5(i). Respondent asserts that the responsive information "was collected, assembled and maintained for the purpose of providing security for the courthouse and judges, and to prevent any criminal acts." Though we agree that this may be the case, we do not believe that these records relate "to the specifications, operating procedures, or location of a security system used to protect public or private property from an act of terrorism or related criminal activity." Accordingly, we conclude that these records are not exempt from disclosure under Rule 12.5(i).

Computer usage and log-in/log-out records

We next address Petitioner's request for computer usage records and computer log-in and log-out records. A special committee considered the release of these records in Rule 12 Decision No. 16-010. In that appeal, Petitioner had requested a judge's computer log-on and log-off times for a two-year time period. The panel noted that the requested information is not the type that judicial officers ordinarily make or maintain in the regular course of business and questioned whether the information existed or would need to be created. The panel concluded that if the report did not exist it did not have to be created.

Following the analysis of Rule 12 Decision No. 16-010, if the requested information does not exist, Respondent does not have to create it. If the information exists, we are unable to conclude how the release of one record indicating whether Respondent was in the building on a specific date would jeopardize Respondent's security against physical injury or jeopardize information or property against theft. Additionally, we do not believe this information "relates to the specifications, operating procedures, or location of a security system used to protect public or private property from an act of terrorism or related criminal activity" so that it is covered by Sec. 418.182(a) of the Government Code.

E-mail and phone call records

Respondent also raises Rule 12.5(b) and (i) as the basis for withholding "e-mails opened or sent" and "phone calls received or made" that reflect the time Respondent left the criminal justice center on a specific date or which reflect that he was in the building until a specific time. As a result

of modern technology that enables individuals to work outside of the office, the time stamp indicating when an email was sent does not necessarily confirm that a person was in fact in the office when the email was sent. Therefore, the release of emails with this information would not jeopardize Respondent's security against physical injury. Respondent did not indicate if records of "phone calls received or made" exist. If they do not exist, they do not have to be created. If they do exist, we do not believe that the release of this information would jeopardizes Respondent's security against physical injury. Accordingly, these records are not exempt under Rule 12.5(b) or 12.5(i).

Conclusion

In summary, we conclude that the responsive records, if they exist, are not exempt from disclosure under Rule 12.5(b) or (i). However, we are mindful of the potential security concerns and risks that judicial officers sometimes face. Therefore, because we have reached this decision without the benefit of reviewing the responsive records, we give Respondent leave to submit any responsive records for our *in camera* review to ensure that they are not exempt from disclosure. If Respondent chooses not to submit the responsive records for our review, they should be released to Petitioner.