

Contact:

Chief Justice Annette Kingsland Ziegler
Wisconsin Supreme Court
(608) 266-1881

FOR IMMEDIATE RELEASE

Madison, Wisconsin (April 30, 2025) — In late June of 2024, the Wisconsin Supreme Court suffered a breach of trust the court had not experienced in its history. The court was shocked to learn on June 26, 2024, that a confidential draft document had been leaked to the press. All seven members of the court condemned the breach.

Because the court does not have an independent law enforcement agency, the court retained the services of an independent investigator to conduct the investigation.

We have been informed by the investigator that the results of the investigation are inconclusive. Attached please find the written report.

#

INVESTIGATION OF THE PLANNED
PARENTHOOD OF WISCONSIN V.
URMANSKI LEAK TO THE MEDIA

April 23, 2025

Investigation Overview

This investigation was initiated to determine how information contained in a confidential draft order was obtained by the media. This report also provides recommendations to enhance Wisconsin Supreme Court document security measures going forward.

The investigative process involved background inquiries, interviews with individuals who had or potentially had access to the draft order and a forensic analysis of computer data.

Sixty-two people were interviewed during the investigation. The interviews included Supreme Court Justices, judicial staff, Supreme Court Commissioners, interns, personnel who accessed the Justice Chambers between June 13, 2024 and June 26, 2024, and any other individuals who may have had knowledge of the draft order prior to the leak.

As part of the investigation, network logs, including individual web histories, shared folder files, individual folders, and emails from all employees with access to the draft order were reviewed.

Printer data was analyzed to identify who may have printed the leaked draft order.

The investigation concluded that the leak of the draft order to the media was likely deliberate. However, no individual could be definitively identified as responsible for the leak.

This investigation has been suspended pending the emergence of new information. All available leads have been thoroughly pursued, and no suspects have been positively identified at this time. The investigation can be resumed as appropriate should additional information become known.

Table of Contents

Background	1-3
Timeline of Leaked Planned Parenthood Draft Order	4-5
Office of Management Services Policies.....	6-9
Investigative Steps.....	10-17
Security Recommendations	18-25

Background

This concerns the Wisconsin Supreme Court and a petition to take jurisdiction of an original action

Petitioners

- Planned Parenthood of Wisconsin, on behalf of itself, its employees, and its patients
- Kathy King, M.D.
- Allison Linton, M.D, M.P.H.
- Maria L.
- Jennifer S.
- Leslie K.
- Anais L.

Respondents, as Class Representatives for all Wisconsin District Attorneys

- Joel Urmanski, in his official capacity as District Attorney for Sheboygan County, Wisconsin
- Ismael R. Ozanne, in his official capacity as District Attorney for Dane County, Wisconsin
- John T. Chisholm, in his official capacity as District Attorney for Milwaukee County, Wisconsin

Issues Presented

- Whether Wisconsin Statute § 940.04, if interpreted to prevent a person from obtaining an abortion in all circumstances except “to save the life of the mother,” violates the person’s inherent right to life and liberty guaranteed by Article I, Section 1 of the Wisconsin Constitution, by unconstitutionally interfering with the person’s right to bodily integrity, autonomy, and self-determination - including the decision of whether and when to have a child.
- Whether Wisconsin Statute § 940.04, if interpreted to prevent a person from obtaining an abortion in all circumstances except “to save the life of the mother,” violates the person’s right to equal protection guaranteed by Article I, Section 1 of the Wisconsin Constitution, by treating people, including those who seek abortion services, differently than people who seek comparable healthcare services, without an adequate state interest.
- Whether Wisconsin Statute § 940.04, if interpreted to prevent physicians from performing an abortion in all circumstances except “to save the life of the mother,” violates the physicians’ rights to equal protection guaranteed by Article I, Section 1 of the Wisconsin Constitution, by treating physicians providing abortion services differently than those providing comparable healthcare services, without an adequate state interest.

- Whether Wisconsin Statute § 940.04, if interpreted to prevent physicians from performing an abortion in all circumstances except “to save the life of the mother,” infringes on the physicians’ fundamental right to liberty guaranteed by Article I, Section 1 of the Wisconsin Constitution, by preventing them from practicing their chosen profession and treating their patients to the full extent of the physicians’ education, training, and ability, consistent with the patients’ needs.

Timeline of Draft Order Leak

June 26, 2024 - An article authored by Jack Kelly was published on WisconsinWatch.org (<https://wisconsinwatch.org>) revealing unreleased information from the Planned Parenthood draft order. The article quotes a single sentence from the draft order and did not provide any photographs or copies of the draft document.

- The June 13, 2024 version of the draft order includes the quote cited in the Wisconsin Watch article: "It is ordered that the petition for leave to commence an original action is granted, this Court assumes jurisdiction over this entire action, and the petitioners may not raise or argue issues not set forth in the petition for leave to commence an original action unless otherwise ordered by the Court."
- The article further mentions that the Court had resolved to deny the intervention efforts by Wisconsin Right to Life, Wisconsin Family Action, and Pro-Life Wisconsin, while allowing these organizations to submit a brief opposing the lawsuit. This information aligns with the June 13, 2024 version of the draft order.

July 2, 2024 - The Wisconsin Supreme Court issued the relevant order.

July 2, 2024 - Jack Kelly of Wisconsin Watch posted a copy of the filed order on his X/Twitter page utilizing the handle, "@byjackekelly".

Office of Management Services Policies

The Wisconsin Court System Employee Manual Provides

No employee shall use confidential information for personal purposes or divulge or release any confidential information that is not, by statute, Supreme Court rule, or policy established by the director, available to members of the general public. However, no retaliatory disciplinary action may be taken against an employee for the disclosure of information that the employee reasonably believes evidences a violation of statute, Supreme Court rule, or policy established by the director.

The Supreme Court of Wisconsin – Director of State Courts Data Access Agreement Provides

As an employee or contractor at the Wisconsin Court System, you may be entrusted with the ability to access confidential, private, or otherwise sensitive Court information. In order to ensure that you clearly understand the important responsibilities connected with this privileged access, you are required to sign this agreement at the beginning of your contract or employment period and also annually. A signature indicates that you have read and understand the contents of this document and agree to adhere.

You are permitted to view confidential or personal Court information only as necessary to accomplish your job responsibilities. You may never access confidential or personal Court records (examples include juvenile records, sealed records, and Court official notes) for personal reasons, nor for any other non-job-related purpose.

You are permitted to view Court users' personal files or documents only as necessary to accomplish your job responsibilities, or if directed in writing to do so by the department manager.

You are permitted to view users' email (both Court email and personal email) only as necessary to accomplish your job responsibilities, or unless directed in writing to do so by the department manager, director, chief staff attorney, or other designated individual.

If you viewed confidential records, personal files, or users' email as part of your job responsibilities, you may not disclose the contents of these records, files, or emails to anyone, except for job-related purposes, or if directed in writing to do so by the department manager.

You will not maintain department documents or data on any non-authorized computer device or network.

You will report to the department manager any knowledge you have regarding system vulnerabilities, attempted break-ins, data breaches, or violations of this data access Agreement by any staff member or contractor.

An employee must protect his or her user IDs and passwords at all times from unauthorized use to access the Consolidated Court Automation Programs (CCAP) network, department databases and any statewide systems used by the department. An employee will not share a user ID or password with another individual, except with authorized and verified CCAP staff as necessary for support purposes.

Requests from Court system managers, supervisors and employees to process transactions outside the department's established policies and procedures must receive the approval of the department manager.

All employees must adhere to the document handling procedures outlined in the sensitive information policy document.

All documents and electronic records not available to the public are to be considered private or sensitive for the purposes of this policy.

The Wisconsin Court System Sensitive Information Handling Policy Provides

Court sensitive documents and information may or may not require labeling. If access to electronic records require a secure login and password, those documents are considered to be Court sensitive documents. This includes information and/or documents that are accessed through a limited-access network drive. The department manager should provide specific guidance on appropriate labeling. If documents or materials do not fall under a category that the department has already identified as being sensitive or containing Personally Identifiable Information (PII), the information should be treated as confidential until a determination is made whether it is actually sensitive material.

Departments may initially receive Courts sensitive information and PII on handwritten and physical documents, which may or may not be later converted to electronic form. Any printed or handwritten materials containing sensitive information should be retained in a locked office or desk, with access limited to those with a business need to retrieve the information.

A file or folder containing Court sensitive information or PII should not be shared with anyone who is not authorized to access this information.

Employees must ensure that any Court sensitive information or PII that is visible on their monitor is safeguarded from the view of others while in use. If the employee is not at his or her workstation, the screen access should be locked and password-protected. Employees should not rely solely on the automatic timeout locking the screen as the means of protecting the information, as there is a delay before the screen is locked.

Written notes or hardcopy/printout and faxes when no longer needed that do not have a records retention policy or are not considered a public record must be disposed of in an appropriate shred/burn bin or shredded using a cross-cut shredder. Certain types of records are subject to a records retention policy which limits the date on which they can be destroyed. These materials should be retained in a secure and locked area and should be confidentially destroyed when they have reached the end of their required retention period.

Discarded computer equipment (including printer/fax machines) must be decommissioned and the hard drive destroyed using a program that permanently eliminates any PII or Courts Sensitive Information. CCAP will be responsible for the appropriation, decommissioning and disposal of information on computers and laptops. Copiers and fax machine decommissioning will be the responsibility of the Court system purchasing officer.

Any computer equipment being decommissioned must be sanitized of any records. If any records were stored on the computer equipment and must be retained, the employee must proactively move those file to a secure network drive and delete the record from the computer hard drive.

Courts sensitive information or PII, whether written, oral, or electronic, is prohibited to be released to other employees or external entities or individuals unless expressly authorized.

The unauthorized release of Court sensitive information, either through malicious intent, or as the result of failure to follow secure handling requirements as outlined in this document, may result in discipline, up to and including dismissal without the right to appeal. The unauthorized release of information is considered a flagrant offense under section 14.8 of the employee manual and is defined as “misuse or abuse of Courts property” in addition to “intentional neglect.”

The review, release, discussion or dissemination of Court sensitive information without a legitimate business purpose or for personal gain may also result in discipline, up to and including dismissal.

The Supreme Court of Wisconsin – Director of State Courts Consolidated Court Automation Programs Policy Regarding Remote Access Provides

In a public setting, the user must log out of the remote access session when not at the device. In all other settings, the user must lock the device or close the remote access session when stepping away from the device. All remote access windows, including the web browser, must be completely closed after each session. No automated processes to keep VPN connections open during idle periods are allowed. Remote access is automatically disconnected after [REDACTED] of continuous activity.

Other than publicly available Court documents, Court information shall not be stored on unencrypted media unless authorized by the Court.

Investigative Steps

Background Inquiries

Background inquiries were conducted for all personnel interviewed. These inquiries included searches of social media accounts and multiple search engines, and the examination of various websites. Particular attention was given to identifying any connections between employees and reporters with a focus on links to the website WisconsinWatch.org (<https://wisconsinwatch.org>) or reporter Jack Kelly.

Interviews

To ensure a fair and unbiased investigation, all personnel were interviewed using consistent questions and when possible, interviews were conducted in person. In cases where the individual to be interviewed was currently employed by the Court, a face-to-face interview was conducted to maintain consistency and thoroughness of the investigative process.

Any deviation from this protocol, such as accommodating special requests to bypass in-person interviews was denied, as this would have demonstrated favoritism and compromised the equal treatment of all personnel involved. The consistency and integrity of the investigation were paramount to ensure that all personnel were treated equally.

Personnel Interviewed

Listed below are the names of 62 individuals who were interviewed. No one interviewed acknowledged having any knowledge of how the leak occurred.

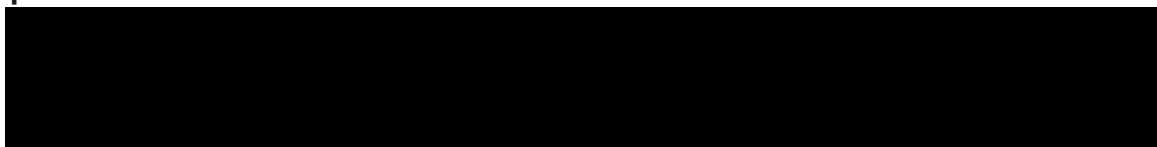
A total of 28 individuals had immediate access to the June 13, 2024 version of the draft order. These individuals were included on the email distribution list for June 13, 2024, through which the leaked draft order was disseminated. The distribution list comprises the following groups: Supreme Court Justices, Supreme Court Judicial Assistant, Supreme Court Law Clerks and Supreme Court Commissioners.

The names of personnel on the distribution list are as follows:

Supreme Court Justices

- Chief Justice Annette Ziegler
- Justice Rebecca Grassl Bradley
- Justice Brian Hagedorn
- Justice Janet Protasiewicz
- Justice Ann Walsh Bradley
- Justice Rebecca Dallet
- Justice Jill Karofsky

Supreme Court Judicial Assistant



Supreme Court Law Clerks

[REDACTED]

Supreme Court Commissioners

[REDACTED]

An additional 18 individuals not included on the distribution list for the draft order were interviewed. Key card entries logged these individuals accessing the Justices' Chambers between June 13, 2024 and June 26, 2024. These people held various roles including facilities personnel, custodial staff, law enforcement, Department of Justice employees, interns and contractors.

The names of these individuals are as follows

[REDACTED]

****Not interviewed as they did not enter Chambers. Their key cards were reissued and used by unknown personnel.*

Thirteen interns assigned to the Justices in June 2024 were interviewed to assess their knowledge of the leak.

The names of the interns are as follows

[REDACTED]

Three additional individuals were interviewed as potential sources of information regarding the leak.

The names of these individuals are as follows

- Director of State Courts Judge Audrey Skiewrawski
- [REDACTED]
- [REDACTED]

Justice Chamber's Security

The Capitol Police conduct daily patrols of the Justice Chambers. [REDACTED]
[REDACTED]
[REDACTED]

Upon examining the Capitol Police dispatch logs for the period of June 13, 2024 through June 26, 2024, there are no recorded instances of unsecured Justice offices.

Analysis of Computer Consolidated Court Automation Programs (CCAP) Data

Computer usage data was preserved, collected and evaluated.

Missing Data

An issue with missing computer data hindered the investigation into the leaked draft order. The relevant computer data, which should have included logs of websites visited from June 13, 2024 through June 26, 2024, was incomplete. It was determined that the only website visitation logs available were from June 26, 2024 and June 27, 2024, not from June 13, 2024 to June 26, 2024 as requested.

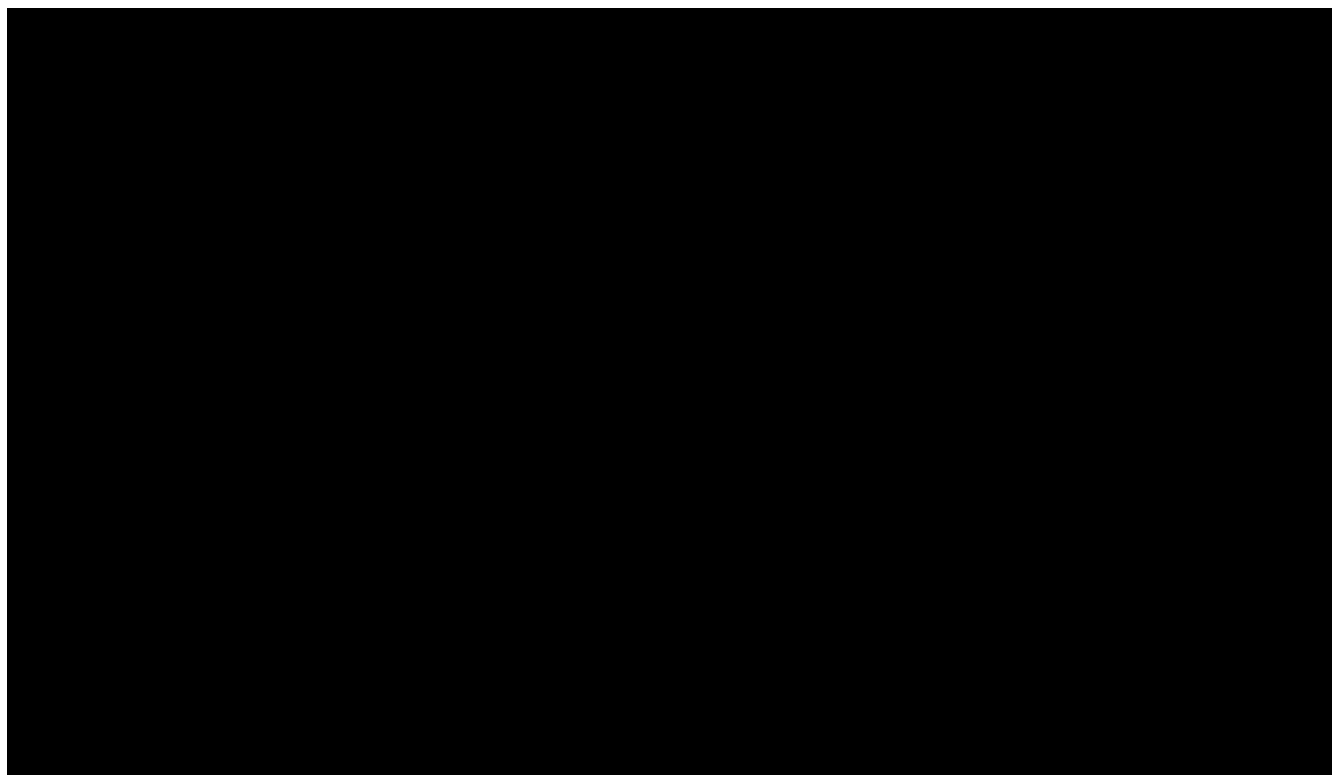
The explanation provided by CCAP Chief Information Officer Tom Flitter reveals a failure in the verification process for the preserved data and highlights an issue with the retention policies regarding website visitation logs. This failure ultimately resulted in the loss of critical information necessary for the investigation.

The lack of complete website visitation logs for the period between June 13, 2024 and June 26, 2024 significantly hampered the ability to thoroughly examine the circumstances surrounding the leak. The issue underscores the importance of proper data management, retention, and verification procedures especially when such information is crucial for ongoing investigations.

Consolidated Court Automation Programs (CCAP) Computer Security

Per SCR 70.01 (2) (d) the Director of State Courts shall have specific responsibility and authority for the court information system.

Internet access for the WI Supreme Court is supported by Information Technology (IT) staff at CCAP. The investigators found that the services provided and current security measures are within acceptable practices for a large organization.



As part of the investigation, network logs including individual web history, shared folder files, individual folders, and emails from all employees with access to the draft order were reviewed.

No evidence was found suggesting the leak was caused by an external threat actor breaching the network or by the document being emailed externally in error.

Printer Usage

Investigators discovered that documents are frequently left unattended on printer trays. Additionally, it was noted that documents have been erroneously sent to incorrect departments for printing. These documents are never retrieved.

On June 25, 2024, Justice Ann Walsh Bradley's law clerk, [REDACTED] printed five documents related to the Planned Parenthood draft order. These documents included the leaked draft order, three documents related to the Justice's opinions, and a document regarding intervenor status. [REDACTED] also printed a document pertaining to Kaul v. Urmanski at this time. [REDACTED] explained the printing was due to the standard operating procedure of Justice Ann Walsh Bradley requiring paper copies of documents.

Key Card Access

Identification cards (ID cards) can be activated for use as electronic key cards. These ID cards are issued by the human resources department, and security access is subsequently managed by the Capitol Police via the Supreme Court Marshal's office.

Access to Restricted Area

During the investigation, it was reported that between June 13, 2024 and June 26, 2024, there were no documented instances of unauthorized access to the Commissioners' Offices on the fourth floor of the Tenney Building. However, there have been past incidents where unauthorized individuals gained access to this restricted floor by entering the elevator along with someone who had key card access.

Intern Information

■ interns assigned to the Justices in June 2024 were interviewed. The majority of interns visited the Justices' Chambers only twice: once at the beginning of their internship and again at the end. One intern worked in the office for several days, and as a result, was granted key card access and a wicourts.gov email account.

Discrepancies were found in the issuance of key cards to interns. Some interns received new key cards, others were given recycled cards not specifically issued to them, and some did not receive a key card at all.

The data shared with interns was primarily limited to publicly available cases for review. However, there were occasions when some interns were informed about the ongoing work of the Court or deduced it on their own.

Analysis of Email Data

Email usage was preserved, collected, and analyzed. The version of the leaked draft order was first circulated on June 13, 2024 and subsequently posted by the media on June 26, 2024.

On three occasions, the draft order was sent to email addresses outside the wicourts.gov email system utilized by the Court. Specifically, it was transmitted on two instances from Law Clerk ■ to Justice Ann Walsh Bradley's personal ■ account. Additionally, Justice Jill Karofsky sent an email containing the draft order to Sergeant Johnson of the Capitol Police.

Law Clerk ██████ said ██████ forwarded the emails containing the draft order to Justice Ann Walsh Bradley's personal email account as that was her standard operating procedure with emails of importance.

The emails show when Justice Ann Walsh Bradley receives emails containing the draft order at her wicourts.gov email address, she forwards it to ██████ who then forwards it to Justice Ann Walsh Bradley's personal ██████ account.

Justice Jill Karofsky explained that she forwarded the draft order to the Sergeant Johnson as the leak could create safety issues that may need to be addressed.

Draft Order Sent to ██████ Account on June 13, 2024 (Prior to Leak)

On June 13, 2024, the draft order, which had been leaked, was forwarded to an email address outside the official wicourts.gov email system. This specific email address was identified as Justice Ann Walsh Bradley's personal email account.

The timeframe of that forwarded email.

- On June 13, 2024 at 4:42 p.m., utilizing the wicourts.gov email system, Commissioner ██████ emailed the Supreme Court Justices, Supreme Court Assistant, Supreme Court Law Clerks, and the Supreme Court Commissioners. The email included the leaked draft order PDF and two additional PDF files.
- On June 13, 2024 at 4:42 p.m., utilizing her wicourts.gov email account, Justice Ann Walsh Bradley forwarded the aforementioned email she received from Commissioner ██████ to her Law Clerk ██████'s wicourts.gov email address. Justice Ann Walsh Bradley did not add any text to the forwarded email. The email included a PDF of the leaked draft order as well as two additional PDF files.
- On June 13, 2024 at 5:08 p.m., utilizing ██████ wicourts.gov email account, Law Clerk ██████ forwarded the email ██████ received from Justice Ann Walsh Bradley's wicourts.gov email account, to Justice Ann Walsh Bradley's personal ██████ account. This email included a PDF of the leaked draft order as well as two additional PDF files.

Draft Order Sent to [REDACTED] Account on June 26, 2024 (After Leak Exposed)

Following the media's request for comment on June 26, 2024, there was one other instance where the leaked draft order was sent to Justice Ann Walsh Bradley's personal [REDACTED] account.

The timeframe of that email.

- On June 26, 2024 at 10:29 a.m., Justice Rebecca Dallet sent an email to Justices Jill Karofsky, Ann Walsh Bradley, and Janet Protasiewicz via their wicourts.gov email addresses. This email contained a PDF of the leaked draft order as well as two additional PDF files.
- On June 26, 2024 at 10:29 a.m., utilizing her wicourts.gov email, Justice Ann Walsh Bradley forwarded this email to her Law Clerk [REDACTED]'s wicourts.gov email address. There was no additional text added by Justice Ann Walsh Bradley in this email. This email contained a PDF of the leaked draft order as well as two additional PDF files
- On June 26, 2024 at 10:33 a.m., utilizing [REDACTED] wicourts.gov account, Law Clerk [REDACTED] forwarded the email [REDACTED] received from Justice Ann Walsh Bradley's wicourts.gov email account, to Justice Ann Walsh Bradley's personal [REDACTED] account. This email contained a PDF of the leaked draft order as well as two additional PDF files. This email was also sent to Law Clerk [REDACTED]'s wicourts.gov email address.

Draft Order Sent to Capitol Police on June 26, 2024 (After Leak Exposed)

On June 26, 2024 at 4:24 p.m., Justice Jill Karofsky emailed Sergeant Johnson of the Capitol Police Department. The email included a PDF of the leaked draft order and two additional PDF files. No accompanying text was provided in the email.

Security Recommendations

These security recommendations collectively aim to enhance the Court's security measures, improve document handling protocols, and safeguard sensitive information against potential risks. Improved document tracking and reduced chances of unauthorized personnel accessing sensitive documents will lead to better overall security. By implementing these recommendations, future incidents regarding leaked information can be investigated more efficiently.

These recommendations address access to secure areas, the transportation and utilization of paper copies, computer usage, email protocols, printer usage, intern guidelines, computer records retention, computer data transfer, tracking of computerized documents, Justice Chambers security, and the importance of maintaining an investigation team on standby.

Key Card Access

- **Current Issue**

Several former employee key cards had not been deactivated. Some of these outdated key cards were reissued to different employees, complicating the tracking of personnel entering secure areas.

- **Recommendation**

Regularly update key card information to ensure accurate tracking and to mitigate unauthorized access. When employees depart or change roles within the organization, it is imperative that key cards are promptly updated to reflect their new status.

Access to Restricted Areas

- **Current Issue**

Unauthorized personnel have been entering secure areas, particularly restricted floors in the Tenney Building. On June 3, 2024, an unauthorized individual accessed the fourth floor where the Commissioner's Office is located. This person was subsequently escorted down to the lobby. The investigation revealed this was not an isolated incident, and breaches of this secure area had occurred in the past.

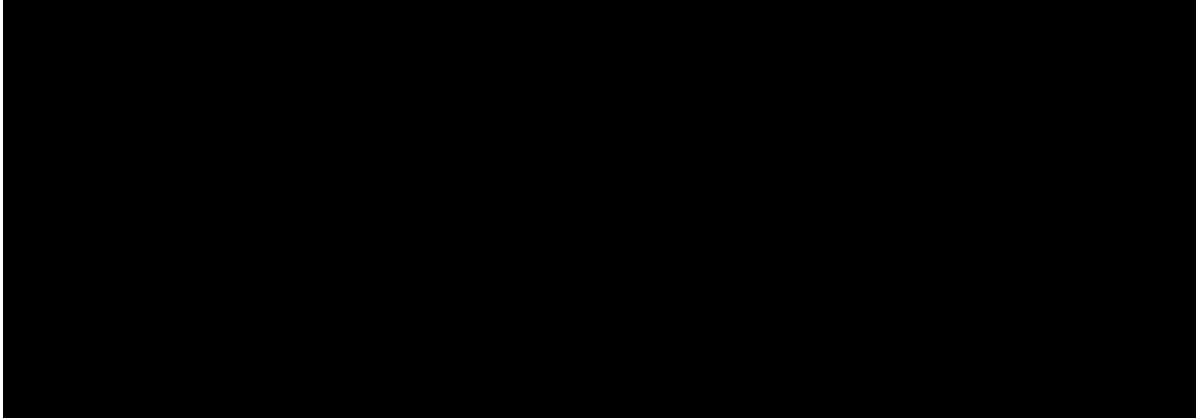
- **Recommendations**

To prevent unauthorized access, be vigilant against "tailgating", also known as "piggybacking". This occurs when an unauthorized person gains access to a restricted area by following closely behind someone who has legitimate access. Ensure that all personnel are aware of this risk and take steps to secure the area immediately after entry.

Ensure that all staff members entering secure areas use their key card to facilitate tracking and to maintain an accurate record of individuals accessing the location.

Transportation of Hard Copies Containing Confidential Information

- **Current Issue**



- **Recommendations**

Ensure that hard copies of confidential documents are delivered in tamper-resistant, sealed packaging to maintain a secure chain of custody.

Use locked or tamper-evident transport containers when utilizing courier services for all documents.

Delivery of Hard Copies Containing Confidential Information

- **Current issue**

When confidential documents are delivered to the Justice's offices and no staff are present, documents are slid under the door of the locked office or left in front of the office door if the document does not fit under the door.

- **Recommendation**

Deliver confidential documents to secure locations only and never leave them unattended outside an office door.

Utilization of Hard Copies Containing Confidential Information

- **Current Issue**

Confidential documents are sometimes left visible and unattended on desks, exposing sensitive information.

- **Recommendation**

Confidential documents should always be stored out-of-sight when not in use.

Destruction of Hard Copies Containing Confidential Information

- **Current Issue**

Employees often delay shredding documents, allowing them to accumulate in bins or boxes for extended periods. These containers are located in individual offices positioned in plain view and accessible to anyone in the office. The primary concern from employees was the limited capacity of the current shredders.

- **Recommendations**

Shred documents immediately when no longer needed. Consider utilizing a document shredding service with locked disposal containers or acquiring larger shredders for higher-volume disposal.

Handling of Non-Confidential Information

- **Current Issue**

Non-confidential documents are often left in open bins or boxes for recycling before being discarded in dumpsters by custodial staff. These dumpsters are located in an unsecure area and can be accessed by anyone, risking exposure of sensitive details such as names, addresses, and case information.

- **Recommendation**

Dispose of all Court-related documents, whether deemed confidential or not, by shredding to protect their integrity and prevent unauthorized access.

Computer Usage

- **Current Issues**

Some personnel share their personal computer login information with subordinates allowing unrestricted access to email accounts.

Some staff members are either unaware of the proper procedures for locking their computers or are unable to do so when stepping away from their desks.

- **Recommendations**

Eliminate the practice of sharing login credentials to maintain system security and data integrity.

Provide training on how and when to lock a computer when not in use.

Email Usage

- **Current Issues**

Some personnel use personal email accounts for Court-related communications. This creates security risks and challenges regarding open records requests for personal emails.

- **Recommendations**

Require employees to use only government-issued email accounts for official communications, reserving personal accounts for private matters.

Printer Usage

- **Current Issues**

Documents are routinely left on the printers.

Due to unnecessary printer options on computers, documents are occasionally and accidentally printed to other departments.

- **Recommendations**

Retrieve documents promptly after printing.

Remove unneeded printer options from Court computers.

Intern Guidelines

- **Current Issue**

Interns are not subject to consistent guidelines regarding internship procedures and access to information.

- **Recommendations**

Establish a consistent on-boarding process for interns to maintain uniformity.

Establish clear policies outlining what information can be shared with interns to ensure consistency.

Intern Key Card Access to Justice Chambers

- **Current Issue**
Some interns are given a key card, others receive a recycled card that was not initially issued to them, and some never get a key card at all.
- **Recommendation**
Given the infrequent presence of interns in the Justice Chambers, it would be wise to implement a policy of not issuing key cards to interns.

Interns Working in the Justice Chambers

- **Current Issue**
Interns typically work remotely but there are occasions when they are present in the Law Clerk's office area where access to sensitive documents is possible.
- **Recommendations**
Interns should always be supervised when they are in the office areas of the Justice's Chambers. Personnel should ensure that all sensitive documents are securely stored and not visible in areas where interns are present.

CCAP Computer Retention Records

- **Current Issue**
Lack of retained data on visited websites hindered the investigation of the leaked draft order.
- **Recommendation**
Develop and enforce policies for preserving computer data immediately following an incident to ensure critical evidence is not lost.

[REDACTED]

- **Current Issue**
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- **Recommendation**
[REDACTED]
[REDACTED]
[REDACTED]

Digital Tracking of Documents

- **Current Issue**

[REDACTED]

- **Recommendation**

While such tracking is not typically required in most business environments, it may be a valuable option for the Court to consider given the specific challenges it faces.

[REDACTED]
[REDACTED]

Incorporating a digital watermark into documents provides an embedded, concealed code designed to monitor and safeguard the document's integrity. This watermark contains essential information about the document's origin, any modifications, and the identities of users who have accessed or edited it. By acting as a unique identifier, the digital watermark facilitates the detection of alterations or unauthorized distribution, ensuring the document remains traceable throughout its lifecycle.

Chambers Security

- **Current Issue**

Doors in the Justice Chambers are occasionally left unsecured, posing a potential security risk.

- **Recommendation**

Ensure that all office doors are locked when the Justice Chambers are unstaffed to maintain security and prevent unauthorized access.

Chambers Access

- **Current Issue**

External contractors are granted access to Justice Chambers to conduct their work.

- **Recommendation**

Ensure that authorized personnel accompany all external contractors while inside the Justice Chambers.

Court Special Investigation Team

- **Current Issue**

The investigation's start was delayed.

When an incident occurs, conducting a prompt investigation is critical to preserving potential evidence and ensuring the integrity of the process.

The document leak incident occurred in June 2024, but the lead investigator was not appointed until August 2024. Additional assistant investigators, requested in August, were not hired until late October 2024. This hiring delay extended the investigation by four months.

The delayed initiation of the investigation resulted in the improper retention of critical computer evidence, compromising the ability to fully examine relevant data.

During the course of the investigation, several involved Court employees had since changed jobs. This required significant efforts to locate them, including tracking individuals who had moved out of state.

- **Recommendation**

It is recommended that the Court establish a dedicated external investigative team capable of immediately investigating incidents. By employing a project-based team, the Court would incur costs only when the team is actively engaged, thus optimizing resource allocation.

To maintain the integrity and impartiality of investigations, the team should operate independently from the Court's daily security operations and activities. This separation helps ensure an unbiased and fair investigative process.

To ensure prompt responses, the investigative team should undergo prior screening, interviews, and vetting, allowing them to begin work immediately when required.

Utilizing an external entity for investigations reinforces public trust in the impartiality and transparency of the process, enhancing the credibility of the Court's response to incidents.