SUPREME COURT OF THE UNITED STATES

STATEMENT OF THE COURT

CONCERNING THE LEAK INVESTIGATION

In May 2022, this Court suffered one of the worst breaches of trust in its history: the leak of a draft opinion. The leak was no mere misguided attempt at protest. It was a grave assault on the judicial process. To meet our obligations as judges, we accept submissions from parties and *amici*, we engage advocates at oral argument, and we publish explanations of our final decisions. All of this we do in the open. Along the way, though, it is essential that we deliberate with one another candidly and in confidence. That phase of the judicial process affords us an opportunity to hone initial thoughts, reconsider views, persuade one another, and work collaboratively to strengthen our collective judgment. It is no exaggeration to say that the integrity of judicial proceedings depends on the inviolability of internal deliberations.

For these reasons and others, the Court immediately and unanimously agreed that the extraordinary betrayal of trust that took place last May warranted a thorough investigation. The Chief Justice assigned the task to the Marshal of the Supreme Court and her staff. After months of diligent analysis of forensic evidence and interviews of almost 100 employees, the Marshal's team determined that no further investigation was warranted with respect to many of the "82 employees [who] had access to electronic or hard copies of the draft opinion." Marshal's Report of Findings & Recommendations 11 (Jan. 19, 2023). In following up on all available leads, however, the Marshal's team performed additional forensic analysis and conducted multiple follow-up interviews of certain employees. But the team has to date been unable to identify a person responsible by

a preponderance of the evidence. *Id.,* at 17. A public version of the Marshal's report is attached.

Recently, this Court consulted Michael Chertoff. Mr. Chertoff is a former Secretary of Homeland Security, Judge of the U. S. Court of Appeals for the Third Circuit, Assistant Attorney General for the Criminal Division of the U. S. Department of Justice, and U. S. Attorney for the District of New Jersey. We invited Mr. Chertoff to assess the Marshal's investigation. He has advised that the Marshal "undertook a thorough investigation" and, "[a]t this time, I cannot identify any additional useful investigative measures" not already undertaken or underway. Statement from Michael Chertoff 1 (2023). A copy of Mr. Chertoff's statement is attached.

The Marshal reports that "[i]nvestigators continue to review and process some electronic data that has been collected and a few other inquiries remain pending." Marshal's Report 2. "To the extent that additional investigation yields new evidence or leads, the investigators will pursue them." *Ibid.* The Marshal and her team will continue to have our full support.

JANUARY 19, 2023

TheChertoffGroup
Enabling A More Secure World

Statement from Michael Chertoff

I was asked by the Chief Justice to independently review and assess the thoroughness of the investigation into the Dobbs draft opinion leak and to identify any additional useful investigative measures as well as actions that would improve the handling of sensitive documents in the future.

My review assessed that the Marshal and her experienced investigators undertook a thorough investigation within their legal authorities, and while there is not sufficient evidence at present for prosecution or other legal action, there were important insights gleaned from the investigation that can be acted upon to avoid future incidents.

Regarding my review, the Court officials provided a detailed account of their investigative process and all documents associated with the investigation, including the interview transcripts and notes of the investigators. The initial round of interviews included a broad swath of employees and were appropriately and professionally conducted. As with most investigations, there were follow-up questions with many employees stemming from the first round of interviews and from forensic evidence. These follow-up interviews were thorough, specific, and ensured all leads were carefully examined. The Court also obtained external expert technical assistance. Throughout my review, the investigators were transparent, cooperative, and available to answer my questions about the process. At this time, I cannot identify any additional useful investigative measures.

The Court investigators will continue following up on leads if more information is learned. In the meantime, the Court has already taken steps to increase security and tighten controls regarding the handling of sensitive documents. Most significantly, the Chief Justice has also directed a comprehensive review of the Court's information and document security protocols to mitigate the risk of future incidents.

In connection with this review, I also recommended the following specific measures:

1. Restricting the distribution of hard copy versions of sensitive documents;
2. Restricting email distribution for sensitive documents;
3. Utilizing information rights management (IRM) tools to better control how sensitive documents are used, edited and shared; and
4. Limiting the access of sensitive information on outside mobile devices.

Office of the Marshal
Supreme Court of the United States
Washington, D.C. 20543

Marshal's Report of Findings & Recommendations
January 19, 2023

On May 2, 2022, Politico published a copy of the draft majority opinion in *Dobbs v. Jackson Women's Health Org., No. 19-1392*. On May 3, 2022, the Chief Justice publicly announced that he had directed the Marshal to launch an investigation into the public disclosure of the draft majority opinion. On May 5, 2022, the Marshal initiated an investigation to determine who made the unauthorized disclosure of the draft majority opinion. The Marshal, in consultation with close advisors at the Court, developed an investigative plan of action. Investigators followed that plan, documented the course of their investigation, and reported the results. Section II of this report captures the material findings and recommendations. The investigative team consists of seasoned attorneys and trained federal investigators with substantial experience conducting criminal, administrative and cyber investigations.

The investigation has determined that it is unlikely that the Court's information technology (IT) systems were improperly accessed by a person outside the Court. After examining the Court's computer devices, networks, printers, and available call and text logs, investigators have found no forensic evidence indicating who disclosed the draft opinion. They have conducted 126

formal interviews of 97 employees, all of whom denied disclosing the opinion. Despite these efforts, investigators have been unable to determine at this time, using a preponderance of the evidence standard, the identity of the person(s) who disclosed the draft majority opinion in *Dobbs* v. *Jackson Women's Health Org.* or how the draft opinion was provided to Politico. Investigators continue to review and process some electronic data that has been collected and a few other inquiries remain pending. To the extent that additional investigation yields new evidence or leads, the investigators will pursue them.

If a Court employee disclosed the draft opinion, that person brazenly violated a system that was built fundamentally on trust with limited safeguards to regulate and constrain access to very sensitive information. The pandemic and resulting expansion of the ability to work from home, as well as gaps in the Court's security policies, created an environment where it was too easy to remove sensitive information from the building and the Court's IT networks, increasing the risk of both deliberate and accidental disclosures of Court-sensitive information. The investigation has identified numerous Court policies and practices that should be improved, some of which are set forth in Section II of this report and are being implemented. A more detailed set of recommendations is included as Annex A to the report; Annex A is not being released to the public because doing so could unwisely expose Court operations and information to potential bad actors. The Justices, assisted by

the Court Officers, will need to assess whether to adopt some or all of the more detailed recommendations.

I. Conduct of the Investigation

The draft majority opinion was circulated on February 10, 2022. Politico published the draft opinion on the evening of May 2. The investigation focused on Court personnel – temporary (law clerks) and permanent employees – who had or may have had access to the draft opinion during the period from the initial circulation until the publication by Politico. In the initial phase, investigators sought to gain an understanding of the details of the opinion circulation process; the Court's policies and training addressing confidentiality; laws, if any, that were potentially violated by the unauthorized disclosure; and IT policies in place concerning the handling of sensitive information. The investigators preserved, collected, and reviewed any forensic information that could be found on the Court's IT systems and conducted formal interviews with Court personnel. The investigative team also enlisted external technical assistance when necessary to examine specific items of evidence.

A. Rules and Court Policies Protecting Confidentiality.

By long-standing tradition, the Court's deliberations are secret. As Justice Powell explained, "[t]he integrity of judicial decision making would be impaired seriously if we had to reach our judgments in the atmosphere of an

ongoing town meeting."[1] Several Court rules and policies prohibit the disclosure of confidential, pre-decisional Court information. The Court presents onset and periodic training to employees on these policies.

(1) The Court's Human Resources Manual.

The Court's Human Resources Manual provides:

> Employees must not disclose or use any confidential information except as required in the performance of official duties or except as expressly permitted by the Court or the employee's supervising Court Officer.
>
> "Confidential information" means any information relating to the Court or its employees that is not made public through means authorized by the Court. Confidential information includes without limitation:
>
> - Non-public information relating to a case, such as the outcome of a case, the vote in a case, the identity of the author of any opinion in a case, and the date on which a decision in any case will be announced;
>
> - The views of any Justice relating to cases or issues that have been before the Court, are currently pending before the Court, or are likely to come before the Court;
>
> - Non-public information related to the Court's policies, procedures, or practices; and
>
> - Non-public personal information about individuals who work at the Court.
>
> A former employee remains bound to the same restrictions on disclosure of confidential information that apply to a current employee, except as modified by the Court or the Court Officer supervising the employee's former office.

[1] *See* Lewis F. Powell, Jr., What Really Goes on in the Supreme Court, in David M. O'Brien, ed., Judges on Judging: Views from the Bench 84 (1997).

> Federal law prohibits the unauthorized disclosure or use of information by federal employees and provides for penalties of termination, fines, or imprisonment for unauthorized disclosure or use of information. *See, e.g.*, 18 U.S.C. §§ 641, 1905, 2071.

S.Ct. Human Resources Manual § 6.03 (Oct. 4, 2021). The Legal Office presents onset and periodic ethics training to all employees and the training addresses the Court's confidentiality requirements and policy.[2]

(2) The Supreme Court Law Clerk Code of Conduct.

The Law Clerk Code of Conduct provides:

> The law clerk owes the appointing Justice, all other Justices, and the Court as an institution, duties of complete confidentiality, accuracy, and loyalty. Justices rely upon law clerks' assistance in exploring issues in pending cases. Justices rely on confidentiality in discussing the performance of their judicial duties and the work of the Court, and they expect and require complete loyalty from their own law clerks and the clerks of all other Justices.
> . . .
> The law clerk, like the Justices, holds a position of public trust and must comply with the demanding standards of that position.
> . . .
> Separate and apart from the duty owed by each law clerk to the appointing Justice is the duty owed by each law clerk to the Court as a body. Each law clerk is in a position to receive highly confidential circulations from the Chambers of the other Justices and other Court offices. All information from all Chambers and Court offices pertaining to the work of the Court is confidential

[2] The HR Manual also states that employees must take guidance from the Code of Conduct for Judicial Employees. *See id.* § 6.01. That code provides that "[a] judicial employee should avoid making public comment on the merits of a pending or impending action and should require similar restraint by personnel subject to the judicial employee's direction and control." Code of Conduct for Judicial Employees, Canon 3D(1). "A judicial employee should not use for personal gain any confidential information received in the course of official duties." *Id.*, Canon 3D(2). "A judicial employee should never disclose any confidential information received in the course of official duties except as required in the performance of such duties. A former judicial employee should observe the same restriction on disclosure of confidential information that applies to a current judicial employee, except as modified by the appointing authority." *Id.*, Canon 3D(3).

> information. "Confidential information" means any information relating to the Court or its employees that is not made public through means authorized by the Court or by the law clerk's appointing Justice, including without limitation:
>
> - the outcome of a case; the vote in a case; the identity of the author of a majority, concurring, or dissenting opinion; the date on which an opinion is to be announced;
>
> - the positions or preliminary ideas or views of any Justice with respect to cases that have been before the Court, are pending before it, or are likely to come before it;
>
> - information relating to the Court's policies, procedures, and practices; and
>
> - personal information about individuals who work at the Court.
>
> Nothing in this Code precludes the reporting of potential misconduct to the law clerk's appointing Justice, the Chief Justice, the Counselor to the Chief Justice, the Legal Counsel, or the Human Resources Director

Law Clerk Code of Conduct, Canon 2. It further provides:

> A law clerk should never disclose to any person any confidential information received in the course of the law clerk's duties, nor should any law clerk employ such information for private gain. A law clerk must maintain all Court-related information in accordance with policies, guidelines, and agreements adopted by the Court's Office of Information Technology.
> . . .
> Except as authorized by the Justice, the clerk must avoid any hint about the Justice's likely action in a pending case. All intra- and inter-Chambers communications are confidential and communications from the Chambers of another Justice enjoy the same protections of confidentiality, including communications from one law clerk to another discussing the work of the Court. The temptation to discuss interesting pending or decided cases among friends, spouses, or other family members, for example, must be scrupulously resisted.

Id., Canon 3. "Any breach of these provisions is prejudicial to the administration of justice and therefore will subject the law clerk to appropriate

sanctions." *Id.*, Compliance. The Chief Justice and the Legal Office discuss the Code of Conduct with all incoming law clerks. All law clerks sign confidentiality agreements stating that they are undertaking positions of trust in the federal government, and that they have read and understand the Law Clerk Code of Conduct and the Court's Non-Disclosure and Information System User Agreement.

(3) The Court's Information Technology Policies.

The Court requires every employee to sign a Non-Disclosure and Information System User Agreement in order to obtain computer access and for each Court-provided mobile device. These documents include key requirements from the Court's Information System User Guidelines.

The Court's Information System User Guidelines state that the standards in that document "apply to all government employees . . . granted access to Court information systems." S.Ct. Info. Sys. User Guidelines § 1.2 (June 2019). The Guidelines state that employees must "[e]nsure [that] unauthorized individuals are not permitted to access [or] view . . . Court Sensitive Information," and "[e]nsure [that] Court Sensitive information is transmitted or stored on approved networks or devices only." *Id.* ¶ 3.1. The guidelines prohibit "[a]llowing Court Sensitive Information to reside on non-Court issued IT assets without proper authorization," and prohibit "[a]ttempting to leave facilities with Court Sensitive information (hard copy or electronic) without

proper authorization." *Id.* "Court Sensitive" information is defined to mean "information whose loss, unauthorized access, or modification could adversely affect the Court's operations, assets, or individuals," and it includes "[c]ert pool memos, bench memos, opinion-related information," and "Court actions prior to official public release."

The HR Manual provides that all employees must comply with all IT policies, including this policy. *See* HR Manual § 6.07 (employees must comply with the Information System User Guidelines).

(4) Code of Conduct for U.S. Judges.

The Code of Conduct for U.S. Judges provides: "A judge should not make public comment on the merits of a matter pending or impending in any court. A judge should require similar restraint by court personnel subject to the judge's direction and control." Code of Conduct for U.S. Judges, Canon 3A(6).

B. Laws Potentially Relevant to the Investigation.

The following federal statutes are potentially relevant to the investigation:

- 18 U.S.C. § 371 prohibits two or more persons from conspiring to commit an offense against the United States or to defraud the United States in any manner or for any purpose.
- 18 U.S.C. § 401 states that "[a] court of the United States shall have power to punish . . . such contempt of its authority . . . as . . . [m]isbehavior of any person in its presence of so near

thereto as to obstruct the administration of justice" and "[m]is-behavior of any of its officers in their official transactions."

- 18 U.S.C. § 641 prohibits the disposition "without authority" of any record or thing of value of the United States.

- 18 U.S.C. § 1030 prohibits intentionally accessing a computer without authorization or exceeding authorized access and thereby obtaining information from any department or agency or the United States.

- 18 U.S.C. § 1503 prohibits "corruptly . . . endeavor[ing] to influence, intimidate, or impede any . . . officer in or of any court of the United States . . . in the discharge of his duty . . . or corruptly . . . influenc[ing], obstruct[ing], or imped[ing], or endeavor[ing] to influence, obstruct, or impede, the due administration of justice."

- 18 U.S.C. § 1905 prohibits disclosure by federal government employees of information that comes to them in the course of their employment that is known by them to be confidential, including the "identity" of "any person."

- 18 U.S.C. § 2071 prohibits unlawful removal of any record filed or deposited with any judicial officer of the United States.

In addition, bills were introduced in the last Congress that would have expressly prohibited the disclosure of confidential Supreme Court information. *See* H.R. 7917 & S. 4455 (117th Cong) (bills to provide for penalties for the unauthorized disclosure of confidential information by Supreme Court employees). Another statute, 18 U.S.C. § 1001 [False Official Statements], has become important to the investigation since all personnel who had access to the draft opinion signed sworn affidavits affirming they did not disclose the draft opinion nor know anything about who did. If the investigators determine any of these personnel lied, they could be subject to prosecution under 18 U.S.C. § 1001.

C. Forensic IT information.

It is unlikely that the public disclosure was caused by a hack of the Court's IT systems. The Court's IT department did not find any indications of a hack but continues to monitor and audit the system for any indicators of compromise or intrusion into the Court's IT infrastructure. The investigators have likewise not uncovered any evidence that an employee with elevated IT access privileges accessed or moved the draft opinion.

The investigative team obtained forensic information from the Court's IT systems in order to identify individuals of interest to the investigation, and to furnish the basis for questioning of employees. In several cases, such forensic information caused investigators to hold multiple interviews with certain employees. The investigative team reviewed the operating system event logs and other logging for artifacts relevant to the draft majority opinion. One initial focus of that review was to determine whether the draft opinion had been moved electronically from the Court's IT system prior to the Politico publication. They found that certain employees emailed the draft document to other employees, with approval. There was no evidence discovered that anyone emailed the draft opinion to anyone else, although technical limitations in the Court's computer recordkeeping at the time made it impossible to rule out this possibility entirely.

The investigators were not able to readily search and analyze all event logs because at the time the system lacked substantial logging and search functions.

The investigators determined that in addition to the Justices, 82 employees had access to electronic or hard copies of the draft opinion.

On February 10, the draft opinion was sent via email to a distribution list consisting of law clerks and permanent personnel who work on opinions. The vote memos were also subsequently sent to this list. There were 70 unique, active users on the distribution list. On March 22, eight more permanent personnel received the draft opinion via email. The investigators also found that two additional permanent personnel accessed the draft opinion electronically by separate means. In sum, the investigators determined that 80 personnel received or had access to electronic copies of the draft opinion.

The draft majority opinion was also distributed in hard copy to some Chambers. The two Chambers personnel who were not on the email distribution list would have had access to the circulated hard copies and to any other copies that were printed in Chambers. Thirty-four personnel confirmed they printed out copies of the draft opinion and four were unsure; many printed out more than one copy. And, as noted in Section D below, in the course of their interviews, several personnel acknowledged that they did not

treat information relating to the draft opinion consistent with the Court's confidentiality policies.

The investigators searched all available logs for evidence of who handled the draft majority opinion after circulation. A few circumstances justified closer inspection, which was conducted but did not result in any solid leads as to the identity of who may have disclosed the document. Consistent with standard policy for most law enforcement agencies, this report does not identify any individuals who received additional scrutiny because (a) certain aspects of the investigation may yield additional pertinent information and (b) in any event, there is not adequate evidence, even applying a preponderance of the evidence standard, to conclude that any particular individual was responsible for the disclosure.

The investigators did not find any logs or IT artifacts indicating that the draft opinion was downloaded to removable media, but it is impossible to rule out.

During the search of logs for networked printers, the investigators discovered very few confirmed print jobs of the draft majority opinion. This is the case for two reasons. First, for some networked printers there was very little logging capability at the time, so it is likely that many print jobs were simply not captured. Second, the investigators learned that many printers in

the building, including some assigned to Chambers, were locally connected printers and not resident and tracked on the Court's networks. This means that the print logs for these printers were stored only locally in the printers' internal memory. These local, desk-side printers typically keep a log of the last 60 documents printed on the printer. The investigators obtained the hard copy print outs of the logs from 46 local printers but found nothing relevant in the limited logs.

The investigators collected Court-issued laptops and mobile devices from all personnel who had access to the draft opinion. To date, the investigators have found no relevant information from these devices.

The Court historically has not issued mobile phones to all employees. However, all employees who were requested to do so voluntarily provided call and text detail records and billing statements for their personal devices for a defined period to the best of their abilities. The investigators reviewed the call and text logs retrieved but found nothing relevant in the limited logs.

D. Interviews.

The investigators to date have conducted 126 formal interviews of 97 personnel. At the initial interviews, the investigators informed all witnesses that they had a duty to answer questions about their conduct as employees; that disciplinary action including dismissal could be undertaken if they refused

to answer or failed to answer fully and truthfully; that the answers provided and any resulting information or evidence could be used in the course of civil or administrative proceedings; and that such information or evidence could not be used against them in any criminal proceedings unless they knowingly and willfully provided false statements. All personnel agreed to be interviewed and many were interviewed more than once.

For the initial interviews with employees, investigators reviewed any available legal research history while bulk requests were pending with the service providers. The purpose was to determine whether an employee might have researched the legality of disclosing confidential case-related information – possibly indicating the person's intention to do so or concern about having done so after the fact. Investigators later obtained, analyzed and confirmed legal research history for all employees directly from the service providers. The investigators did not find anything suspicious or relevant in these records.

At the conclusion of the initial interviews, each employee was asked to sign an affidavit, under penalty of perjury, affirming that he or she did not disclose the *Dobbs* draft opinion to any person not employed by the Supreme Court, did not disclose to any person not employed by the Supreme Court any information relating to the *Dobbs* draft opinion not made public through means authorized by the Court, and had provided all of the pertinent information known to him or her relating to the disclosure or publication of the *Dobbs* draft

opinion. Each employee was then asked to swear to the truth of the statements in the affidavit before a Notary Public. Each of these employees signed a sworn affidavit. A few of those interviewed admitted to telling their spouses about the draft opinion or vote count, so they annotated their affidavits to that effect. If investigators later determine any personnel lied to the investigators, those personnel would be subject to prosecution for a false statement in violation of 18 USC § 1001.

The interviews provided very few leads concerning who may have publicly disclosed the document. Very few of the individuals interviewed were willing to speculate on how the disclosure could have occurred or who might have been involved. The investigators found most of their leads in the IT forensics discussed previously. Nevertheless, the investigators diligently followed up on leads related to several personnel.

Some individuals admitted to investigators that they told their spouse or partner about the draft *Dobb*s opinion and the vote count, in violation of the Court's confidentiality rules. Several personnel told investigators they had shared confidential details about their work more generally with their spouses and some indicated they thought it permissible to provide such information to their spouses. Some personnel handled the *Dobbs* draft in ways that deviated from their standard process for handling draft opinions.

Investigators carefully evaluated the statements and conduct of personnel who displayed attributes associated with insider-threat behavior – violation of confidentiality rules, disgruntled attitude, claimed stressed, anger at the Court's decision, etc. – and also weighed behavior and evidence that would tend to mitigate any adverse inferences. Investigators also carefully evaluated whether personnel may have had reason to disclose the Court's draft decision for strategic reasons.

Investigators looked closely into any connections between employees and reporters. They especially scrutinized any contacts with anyone associated with Politico. Investigators also assessed the wide array of public speculation, mostly on social media, about any individual who may have disclosed the document. Several law clerks were named in various posts. In their inquiries, the investigators found nothing to substantiate any of the social media allegations regarding the disclosure.

E. Outside Assistance.

The investigative team requested outside technical assistance on a number of matters. The investigators obtained a forensic examination of the digital image of the draft opinion that was posted on Politico's website to compare against exemplars obtained from Court printers and copiers. There was nothing of evidentiary value that could be gleaned from the electronic copy of the draft opinion when compared against the exemplars.

The investigative team also provided a printer that had been issued to an employee for use at home for analysis to determine if it had any print logs resident in the printer's internal memory. The lab attempted to examine the internal memory chip but was not able to retrieve any logs.

The investigative team received outside assistance with a fingerprint analysis of an item relevant to the investigation. That analysis found viable fingerprints but no matches to any fingerprints of interest.

The investigators also received outside assistance in reviewing the findings of our investigators pertaining to the operating system event logs.

II. General Findings and Recommendations.

At this time, based on a preponderance of the evidence standard, it is not possible to determine the identity of any individual who may have disclosed the document or how the draft opinion ended up with Politico. No one confessed to publicly disclosing the document and none of the available forensic and other evidence provided a basis for identifying any individual as the source of the document. While investigators and the Court's IT experts cannot absolutely rule out a hack, the evidence to date reveals no suggestion of improper outside access. Investigators also cannot eliminate the possibility that the draft

opinion was inadvertently or negligently disclosed – for example, by being left in a public space either inside or outside the building.

Assuming, however, that the opinion was intentionally provided to Politico by a Court employee, that individual was evidently able to act without being detected by any of the Court's IT systems. If it was a Court employee, or someone who had access to an employee's home, that person was able to act with impunity because of inadequate security with respect to the movement of hard copy documents from the Court to home, the absence of mechanisms to track print jobs on Court printers and copiers, and other gaps in security or policies.

The investigative team made general findings and recommendations for restricting and managing access to Court-sensitive materials, improving training, and improving IT capabilities. They are listed below. More detailed recommendations are included in Annex A, which, as previously noted, will not be made public. Many of these are underway and will be completed as soon as practicable.

1. Too many personnel have access to certain Court-sensitive documents. The current distribution mechanisms result in too many people having access to highly sensitive information and the inability to actively track who is handling and accessing these documents. Distribution should be more

tailored and the use of hard copies for sensitive documents should be minimized and tightly controlled.

2. Aside from the Court's clear confidentiality policies and the federal statutes outlined above, there is no universal written policy or guidance on the mechanics of handling and safeguarding draft opinions and Court-sensitive documents, and practices vary widely throughout the Court. A universal policy should be established and all personnel should receive training on the requirements.

3. The Court's current method of destroying Court-sensitive documents has vulnerabilities that should be addressed.

4. The Court's information security policies are outdated and need to be clarified and updated. The existing platform for case-related documents appears to be out of date and in need of an overhaul.

5. There are inadequate safeguards in place to track the printing and copying of sensitive documents. The Court should institute tracking mechanisms using technology that is currently available for this purpose.

6. Many personnel appear not to have properly understood the Court's policies on confidentiality. There should be more emphasis on training so that all personnel fully understand the policies.

7. Bills were introduced in the last Congress which would expressly prohibit the disclosure of the Supreme Court's non-public case-related information to anyone outside the Court. Consideration should be given to supporting such legislation.

In time, continued investigation and analysis may produce additional leads that could identify the source of the disclosure. Whether or not any individual is ever identified as the source of the disclosure, the Court should take action to create and implement better policies to govern the handling of Court-sensitive information and determine the best IT systems for security and collaboration.