Securing the JUSTIN System

Access and Security Audit at the Ministry of Justice

OFFICE OF THE
Auditor General
of British Columbia

About Our Office

- The Auditor General is the independent auditor of the Legislative Assembly of British Columbia

- Reports to the Legislative Assembly, not to the government of the day

- Conducts both financial audits and performance (or "value for money") audits

OFFICE OF THE
Auditor General
of British Columbia

Background

- JUSTIN is an integrated system for managing and administering the criminal justice process

- Contains 15 years of adult and youth case information

- Contains some of most sensitive information in government

OFFICE OF THE
Auditor General
of British Columbia

Background

Criminal justice process

Policing
- Investigates crimes
- Recommends charges

Crown Counsel
- Approves charges
- Prosecutes offenders

Judiciary
- Schedules cases
- Tries cases

Court Services
- Maintains court registry
- Manages and administers court documents

Corrections
- Provides community supervision for released offenders
- Custody for serious offenders

OFFICE OF THE
Auditor General
of British Columbia

Background

Reports to Crown Counsel (RCCs) include:

- Narratives of police investigations
- Accused information
- Witness 'will say' statements
- Witness and victim contact information
- Charge assessments

OFFICE OF THE
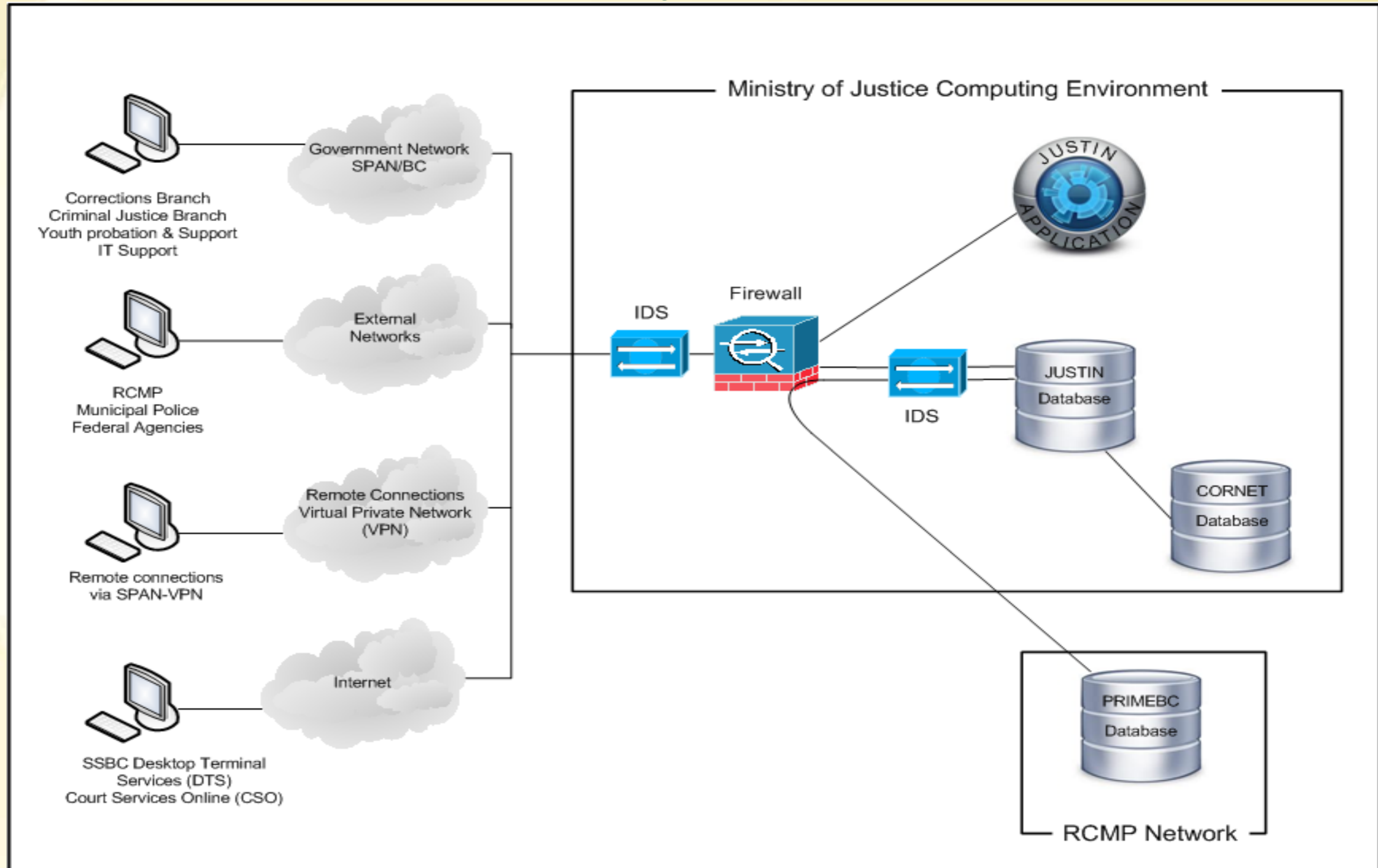Auditor General
of British Columbia

Background

Over 3,300 JUSTIN users have access to RCCs

- RCMP and Municipal Police
- Ministry of Justice
  - Criminal Justice Branch
  - Corrections Branch
- Ministry of Children and Families
- Federal Crown Counsel

OFFICE OF THE
Auditor General
of British Columbia

Background

A simplified view of the JUSTIN computing environment

Objective

Protection of JUSTIN information:

- Is the system adequately secured from internal and external threats?

- Are JUSTIN information breaches likely to be discovered and effectively managed?

Conclusion

- JUSTIN information is not adequately protected from internal or external threats.

- It is unlikely that unauthorized access or removal of copied information will be discovered.

- Risks from wrongful disclosure are unlikely to be mitigated.

OFFICE OF THE
Auditor General
of British Columbia

Key Findings

1. The JUSTIN environment is not secured from external threats

2. There is excessive user access

3. Highly sensitive data is not locked down

4. No visibility or control over information leaving the organization

5. Proactive response is not possible as breaches could be undetected

OFFICE OF THE
Auditor General
of British Columbia

Key Findings

1) The JUSTIN environment is not secured from external threats

- Assessed security controls in IT components including:
    - Firewall and network components
    - Servers
    - Operating system
- Network penetration testing

OFFICE OF THE
Auditor General
of British Columbia

Key Findings

2) There is excessive user access

- 3,300 users with access to almost all RCCs

- Access is not based on 'Need to Know'

- Users can access:

  - RCC narratives

  - Victim and witness contact information

  - Witness "will say" statements

OFFICE OF THE
Auditor General
of British Columbia

Key Findings

3) Highly-sensitive data is not locked down

- Highly-sensitive adult RCCs

- Youth RCCs

- RCCs pertaining to:

  - Sealed court cases

  - Pardoned individuals

OFFICE OF THE
Auditor General
of British Columbia

4) No visibility or control over information leaving the organization

- User actions are not sufficiently tracked

- User actions are not monitored

- For example users are able to:

    - Print RCCs and/or save to file

    - Search by name

5) Proactive response is not possible as breaches could be undetected

- There are no methods to detect:
    - Compromised accounts
    - Unauthorized access

- Insufficient collection of user activity to allow proper investigation

OFFICE OF THE
Auditor General
of British Columbia

Recommendations

- 100 recommendations reported to ministry management
- 5 key recommendations summarized in public report:

1. Controls in network and system components should be reviewed, reconfigured, documented, and better managed.

2. User access to JUSTIN information should be granted and managed based on the principle of 'need to know'.

3. Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring.

4. More effective audit trails and tools should be in place.

5. An effective monitoring program should be in place to enable proactive detection of unauthorized access and removal of copied JUSTIN information.

OFFICE OF THE
Auditor General
of British Columbia

Looking Ahead

- Ministry action plan

- Progress will be monitored

- Follow-up report

OFFICE OF THE
Auditor General
of British Columbia

Further Resources

Visit www.bcauditor.com to:

- read the full report

- subscribe to our e-notification service and be notified when we release a report

- see our "Work in Progress"

- learn more about the Office

- provide your feedback on this report and/or suggestions for further audits

OFFICE OF THE
Auditor General
of British Columbia