Justice and Solicitor General—Justice Online Information Network System Follow Up

SUMMARY

What we examined

In 2012, we audited IT security for the transfer of traffic fines information between the government's Justice Online Information Network system and its external partners' systems. We examined the method the department used to receive the data, summarize and report on it and send summaries of fines back to ticketing partners and municipalities.

What we found

Unsecured transmission of ticket data
In 2012, we found that the department sent ticket data over the internet using an unsecured network protocol called FTP (file transfer protocol). FTP sends data in clear text and unencrypted over the internet. Ticket data includes details such as the driver's licence number, name, address, date of birth and the specifics of the fine. The department also uses the JOIN application to produce and send reports to police services and to reconcile tickets they have sent to Justice. These reports were also sent to municipalities over the internet, in the same unsecured fashion.

Data could be intercepted
Transmitted over the internet without security controls to protect it from unauthorized access, this information could be compromised by hackers who use relatively common techniques such as:

- packet capture or data sniffing attack—A network intruder could simply connect to one of the many internet network nodes[1] that data passes through on its way to the servers and back, and could steal the data
- bounce "man-in-the-middle" attack—An intruder could modify the data passing through the internet node and then allow it to continue to its destination, for malicious or fraudulent purposes

Non-compliance with the department's security policy
The department did not follow its own security policies, which clearly state that personal data transmitted outside of the government must be protected from unauthorized access. We did not find any occurrences where data had been accessed by an unauthorized party. However, the risk was high that this could occur and the department would not know if or when it had occurred.

We immediately recommended that the department improve the security over data transmitted over the internet. Because of the sensitivity of this finding and the potential for loss of confidential information, we exercised our discretion to not publicly report our finding in 2012. We did not want to create a beacon for hackers to focus attacks on this vulnerability. In response to our recommendation in 2012, management informed us that a high priority project was underway to securely transmit ticket data.

[1] The internet is a global system of interconnected computer networks that are linked by a broad array of electronic technologies and devices, commonly referred to as nodes. When data is transmitted from one point or "node" on the internet, it may pass through various other devices' nodes along the way to its destination.

During our 2013 audit of the department, we followed up on management's plans and actions to implement a secure file transfer method of ticket data for its JOIN application. Management advised us that, as of March 2013, it had implemented the necessary changes to its systems and its partner systems to ensure that all traffic ticket data would be transmitted using a secure method that would not allow for unauthorized access.

We tested the design and operating effectiveness of the new JOIN secure transfer system and confirmed that the department has resolved this critical security exposure. We now consider the 2012 recommendation to be implemented.