



MINISTRY OF SOCIAL DEVELOPMENT

Te Manatū Whakahiato Ora

Bowen State Building, Bowen Street, Wellington 6011, PO Box 1556, Wellington 6140 • Telephone: 0-4-916 3300 • Facsimile: 0-4-918 0099

16 NOV 2012

Mr Josh Levent
fyi-request-615-927b4e24@requests.fyi.org.nz

Dear Mr Levent

Thank you for your email received on 23 October 2012 requesting, under the Official Information Act 1982, the following information:

"1. All reports to the Ministry and to the Ministry's agencies (and any staff member therein) regarding or containing an assessment of the IT security at the Ministry and/or any of its agencies in the last 5 years. This includes but is not limited to:

- A report made by Dimension Data in April last year*
- Any internal reports made by staff*
- Any reports made by IT contractors while implementing any IT solution operating on an MSD network*

Please release the full text of these reports, who they were submitted by, the date they were submitted, who they were submitted to (a full list of people who received a copy of the report), and what actions related to information security were taken as a result (if any).

2. I request that you release all information security plans in place over the last 5 years at the Ministry and all of its agencies, including the full text of such plans, the date at which such plans were adopted, the date at which they were superseded by a newer plan, and the extent to which they comply with the International Standards Organisation Information Security Management Standard (AS/NZS ISO/IEC 27001:2006)."

As you may be aware, on 2 November 2012 the Ministry of Social Development released the independent report by Deloitte into the security breach of Work and Income kiosks. This report is publicly available at www.msd.govt.nz.

The *Ministry of Social Development Kiosk Review* by security-assessment.com, a subsidiary of Dimension Data, dated 26 April 2011, was considered by Deloitte during the review. Please find enclosed a copy of this report.

Some information has been withheld under 6(c) of the Official Information Act where making that information available would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences.

This includes any information that details particular methods that could be used to interrogate the Ministry systems, identify system defects, and if released could help others to design ways of inappropriately or illegally accessing the Ministry's systems.

Section 9(2)(k) of the Act is also being applied to prevent the disclosure or use of official information for improper gain or improper advantage. I consider that the public interest is met through the information that is being released to you and the Deloitte report that is available online.

Information has also been removed from the report under section 9(2)(a) of the Act protect the privacy of individuals. I consider that in this instance, the public interest is met through the information that is being provided in the report and withholding the names of these individuals does not detract from this.

I am refusing your request for all information regarding security testing, any reports made by IT contractors while implementing any IT solution operating on the Ministry's network, and all information security plans in place over the last five years under sections 6(c) and 9(2)(k) of the Act. Again, I consider that the public interest is met through the information that is being released to you and the Deloitte report that is available online.

I hope you find the report helpful. You have the right to seek an investigation and review of my response by the Ombudsman, whose address for contact purposes is:

The Ombudsman
Office of the Ombudsman
PO Box 10-152
WELLINGTON 6143

Yours sincerely



MW Marc Warner
Deputy Chief Executive, People, Capability and Resources



security-assessment.com

Security-Assessment.com
Lumley House 3-11 Hunter Street
Wellington
Tel: +64 9 302 5093
Fax: +64 9 302 5023

Ministry of Social Development

Kiosk Review

Complete For Comment

Security-Assessment.com Reference:	20042011-9
Version Number and Status:	0.2 Complete For Comment
Publication Date:	26/04/2011
Security Classification:	Confidential

RELEASED UNDER THE OFFICIAL INFORMATION ACT



Standard Notices

Commercial in Confidence

The material contained in this document is confidential and proprietary to Security-Assessment.com and its intended recipient. The material will be held in the strictest confidence by the recipient(s) and will not be used, in whole or in part, for any purpose other than the purpose for which it is provided without prior written consent by Security-Assessment.com. In no event shall Security-Assessment.com be liable to anyone for direct, special, incidental, collateral or consequential damages arising out of the use of this material, to the maximum extent permitted under law.

Contact for copies:

To obtain a copy of this document and to be added to the distribution list so that you receive all updates to it contact the document author.

Document Revision History

Version	Date	Change	Authoriser
0.1	20/04/2011	Document Creation	section 9(2)(a)
0.2	26/04/2011	Document Review	section 9(2)(a)

OFFICIAL INFORMATION ACT
 UNDER THE ACT
 RELEASED



Table of Contents

1.	Summary	4
1.1.	Executive Overview	4
1.2.	Project Scope	5
1.3.	Project Summary	5
1.4.	Summary of Findings	5
1.5.	Key Recommendations	6
2.	Kiosk Review Summary	7
2.1.	Kiosk Review – Ministry of Social Development	7
3.	Technical Details – Kiosk Review	10
3.1.	Technical Details – Ministry of Social Development	10
3.1.1.	section 6(c)	10
3.1.2.	Lack Of Network Separation	12
3.1.3.	section 6(c)	14
3.1.4.	15
3.1.5.	16
3.1.6.	17
5.	18
6.	Appendix B: Online References	19

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1. Summary

1.1. Executive Overview

This report is a complete for comment report comprised of the outcomes of testing undertaken on the Ministry of Social Development Kiosk deployment. The purpose of testing was to review the Kiosk platform for potential security vulnerabilities and provide advice.

This reviewed was carried out during April 2011. Testing was performed from the perspective of a malicious Kiosk user who was attempting to compromise or otherwise harm the Kiosk terminal. Specific focus was paid toward being able to escape the Kiosk platform and access underlying OS or network resources.

Security testing of the Kiosk platform discovered multiple security findings which pose a level of concern. Discovered findings are not representative of a publicly accessible Kiosk terminal and are considered contrary to best practice. The developed Kiosk solution does not contain adequate security controls in order to meet security standards, and additional changes are required.

The most pressing security issue discovered is the lack of network separation of segregation within the environment. The Kiosk terminals are currently directly connected to the MSD corporate network and share the MSD corporate domain controller. This lack of separation means that the Kiosk terminal has the same level of authority and access as corporate MSD employees. This introduces an inherent level of risk as it could allow for a member of the public to gain access to MSD network resources and services. Physical network separation is strongly recommended, and the current solution should not be deployed into a production environment before network separation is achieved.

This report contains recommendations to increase the current level of security deployed by the Kiosk terminal. Recommendations should be integrated into the currently deployed Operating System image used by the Kiosk. System hardening recommendations made within his report will help to increase the level of security deployed by the Kiosk and will help to defend against attack.

Physical access to any desktop computer will undoubtedly result in the compromise of the desktop, even after significant investment in host hardening. This is due to the nature and design of modern operating systems and the level of trust given to local users. Fundamental changes need to be made to the MSD Kiosk environment to mitigate the current security concerns. The Kiosk should be designed to be within a sandboxed environment which does not have any access to MSD network resources. Ideally this should be achieved through the implementation of a separate network environment which does not share any physical hardware as the MSD corporate network. In the event that the Kiosk is compromised, there should be no additional information, access or privileges to be gained. A secure sandboxed environment would mitigate the level of risk present and limit a malicious user to only be able to compromise Kiosk host itself.

It is our consideration that the testing has been completed in a thorough, professional, and comprehensive fashion. The establishment of remediation activities and further security layers will enable the client to have a higher level of confidence in the environment proceeding forward.



1.2. Project Scope

The following was within the scope of this security audit:

- Kiosk Review: A review of the MSD Kiosk terminal in accordance to best practice and security guidelines regarding public access terminals.

1.3. Project Summary

Testing was conducted from the Ministry of Social Development offices in Wellington. Testing was performed during work hours without any special conditions. The testing was conducted against the Windows XP Kiosk image currently deployed.

1.4. Summary of Findings

Total Vulnerabilities	Severity	Description
	CRITICAL	Critical severity findings allow a remote user to compromise multiple components of a project or solution.
	URGENT	Urgent severity findings relate to a compromise of a component of a project or solution.
	MEDIUM	A medium severity finding relates to a disclosure of non-sensitive information to external third parties.
	MINOR	Minor severity findings contradict security best practice and have minimal impact on the project or solution.
	LOW	Low severity findings relate to housekeeping issues or configuration settings.



1.5. Key Recommendations

While recommendations for individual issues identified have been detailed in the technical section of this document, Security-Assessment.com recommends Ministry of Social Development conduct the following approach to improve the security of the environment:

- Implement remedial actions for the critical / urgent priority issues identified within the technical details of this report;
- Implement network separation as soon as possible using alternative physical hardware such as an additional Firewall. Network separation should be implemented to ensure the Kiosk terminal does not have access to any MSD corporate resources or network services;
- Further restrict the Kiosk environment by implementing the recommendations made within his report.

section 6(c)

- section 9(2)(k)

RELEASED UNDER THE
OFFICIAL INFORMATION ACT



2. Kiosk Review Summary

2.1. Kiosk Review – Ministry of Social Development


Ref No	Severity	Issue	Details	Impact	Recommendation
3.1.1	CRITICAL	section 6(c) section 9(2)(k)			
3.1.2	CRITICAL	Lack Of Network Separation	Kiosks are connected directly to the MSD network and are granted access to network resources and shares as a standard domain user.	The Kiosk appliance is directly connected to the MSD corporate network and is a user of the network. This domain is shared by all MSD desktops, laptops and servers.	The Kiosk terminal needs to be separated from the MSD corporate environment either physically or virtually.



Ref No	Severity	Issue	Details	Impact	Recommendation
3.1.3	CRITICAL	Sensitive Documents Accessible From Kiosk	Security-Assessment.com was able to access documentation stored on open shares within the MSD environment. Documentation was found which included medical and drug test results, credentials stored in plaintext and recorded help desk calls.	A malicious user with access to the operating system of the Kiosk is able to gain access to sensitive information kept within the MSD network, including medical and drug test results.	Restrict all network resources that are available from the Kiosk at a network level. Ideally, the Kiosk should be unable to access any MSD network resources.
3.1.4	CRITICAL				
3.1.5	CRITICAL			section 6(c) section 9(2)(k)	

OFFICIAL INFORMATION



Ref No	Severity	Issue	Details	Impact	Recommendation
3.1.6		section 6(c) section 9(2)(k)			

OFFICIAL INFORMATION ACT
PRELEASED UNDER THE ACT



3. Technical Details – Kiosk Review

section 6(c) Pages 10 to 18
section 9(2)(k)

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

6. Appendix B: Online References

The following links are references to security guides and other links for reference in relation to issues discussed in this document.

- Kioware Kiosks
<http://www.kioware.com>
- Site Kiosk - Provisio:
<http://www.sitekiosk.com>
- Disable Software Restriction Policies:
<http://blogs.technet.com/b/markrussinovich/archive/2005/12/12/circumventing-group-policy-as-a-limited-user.aspx>

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

