Australian Government

Department of Foreign Affairs and Trade

EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT *No.* 447
Recommendation 8 to Department of Foreign Affairs and Trade

31 August 2015

The Secretary
Joint Committee of Public Accounts and Audit
Suite R1.108
Parliament House
CANBERRA ACT 2600

Dear Secretary

Thank you for the opportunity to comment formally on recommendation 8 of the JCPAA report 447 – with reference to ANAO Audit Report No50 2013-14 - Cyber Attacks: Securing Agencies' ICT Systems.

In 2013 the Department of Foreign Affairs and Trade (DFAT) was appropriated funds to refresh and enhance the department's Information and Communications Technology (ICT) infrastructure through major capital work programs known as the International Communications Network (ICN) and the Passport Redevelopment Program. Through these programs the department has been progressively modernising and enhancing its ICT infrastructure, whilst continuing to increase compliance with the top four Strategies to Mitigate Targeted Cyber Intrusions.

The complexity and geographical dispersion of our systems presents challenges to meeting all of the controls stipulated in the top four strategies. Of the 16 controls, DFAT is fully compliant with nine controls; partially compliant with the remaining seven controls, three of which will reach full compliance at the completion of the ICN and PRP capital work, and the remaining four are partially mitigated through policy and procedural controls.

DFAT is committed to delivering robust and secure ICT services for Australian Government business domestically and overseas and will continue to enhance its cyber security posture in accordance with ISM requirements and the department's risk exposure.

Response to the recommendation(s)

Recommendation No. 8 paragraph 5.69

1.1. The Top 4 mandatory controls

1.1.1. *ISM 2015 control 1353*

Agencies, at a minimum, must implement the controls indicated in the following table on all systems able to receive emails or browse web content originating in a different security domain.

TOP 4 CONTROLS		
Mitigation strategy	**Chapter and section of ISM**	**Control numbers**
Application whitelisting	Software Security—Application Whitelisting	0843, 0846, 0955, 1391, 1392
Patch applications	Software Security—Software Patching	0300, 0303, 0304, 0940, 0941 1143, 1144
Patch operating systems	Software Security—Software Patching	0300, 0303, 0304, 0940, 0941, 1143, 1144
Restrict administrative privileges	Access Control—Privileged Access	0445, 0985, 1175
	Personnel Security for Systems—Authorisations, Security Clearances and Briefings	0405

1.2. Application whitelisting

1.2.1. *ISM 2015 control 0843*

Agencies must use an application whitelisting solution within SOEs to restrict the execution of programs and DLLs to an approved set.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT reconfigured the Application Whitelisting policies (AppLocker) in October 2014 to further strengthen whitelisting compliance by including the management of DLLs on the desktops. DFAT is still working to address the compliance on servers. There are two initiatives underway to address whitelisting on servers. The solution for the Windows Server 2012 R2 will be delivered by end of January 2016 and for Windows server 2008 R2 will be delivered by end of March 2016.
The current Australian Passports Office (APO) Microsoft server environment has application whitelisting turned on in audit mode only. Application Whitelisting for

the APO production environment will be fully implemented by the first quarter of 2016.

1.2.2. *ISM 2015 control 0846*

Users and system administrators must not be allowed to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

Standard Users are not able to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.

System administrators are currently exempt from application whitelisting mechanisms on Desktops, as the current application whitelisting product (Applocker) cannot natively restrict Administrators from disabling Application Whitelisting controls. DFAT are implementing a new Role Based Administration model that will limit the number of administrators that can administer desktops and servers to a minimum. This work is currently in progress and will be completed by the December 2015. This will limit the number of administrators to a small number of staff that have the ability to circumvent application whitelisting mechanisms. The actions of these administrators are actively audited through a third party product to maintain positive control of Application Whitelisting.

1.2.3. *ISM 2015 control 0955*

Agencies must implement application whitelisting using at least one of the methods: • cryptographic hashes • publisher certificates • absolute paths • parent folders.

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

Application Whitelisting is implemented on Desktops using Parent Folders, Absolute Paths and Cryptographic Hashes. As stated with control 0843, the solution for the Windows Server 2012 R2 will be delivered by end of January 2016 and for Server 2008 R2 will be delivered by end of March 2016 and the implementation on servers will use at least one of these controls. Application Whitelisting for the APO production environment will be fully implemented by the first quarter of 2016.

1.2.4. *ISM 2015 control 1391*

When implementing application whitelisting using parent folder rules, file system permissions must be configured to prevent users and system administrators from adding or modifying files in authorised parent folders.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

The Whitelisting controls prevent standard users from adding or modifying files in authorised Parent Folders, although a small number of Administrators can.

This cannot be implemented effectively for Administrators using the current Application Whitelisting product. Current mitigation is to limit the number of Administrators, through the Role Based Administration (RBA) plan, who will have the ability to add or modify files in authorised parent folders on desktops and servers. Administration accounts will be actively audited through a third party product to maintain positive control of Application Whitelisting.

1.2.5. *ISM 2015 control 1392*

When implementing application whitelisting using absolute path rules, file system permissions must be configured to prevent users and system administrators from modifying files that are permitted to run.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

The Whitelisting controls prevent standard users from adding or modifying files in authorised parent folders, although a small number of Administrators can.

This cannot be implemented effectively for administrators using the current Application Whitelisting product. Current mitigation is to limit the number of Administrators, through the Role Based Administration (RBA) plan, who will have the ability to add or modify files in absolute paths on desktops and servers. Administration accounts are actively audited through a third party product to maintain positive control of Application Whitelisting.

1.3. Patch applications and Operating systems

1.3.1. *ISM 2015 control 0300*

High Assurance products must only be patched with ASD approved patches using methods and timeframes prescribed by ASD.

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

Any High Assurance products that DFAT use are patched with ASD approved patching methods and timeframes.

1.3.2. *ISM 2015 control 0303*

Agencies must use an approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches as well as the processes used to apply them.

DFAT Compliance status = ***Compliant***

Statement of compliance or detailed plan of necessary activity to achieve compliance:

The process ensuring the integrity, authenticity and application of patches is imbedded in the DFAT ICT Change Management process.

1.3.3. *ISM 2015 control 0304*

Operating systems, applications and hardware devices that are no longer supported by their vendors must be updated to a vendor supported version or replaced with an alternative vendor supported version.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT have secured NPP funding from Government to bring the department's ICT infrastructure up to date with contemporary technology, including operating systems, applications and hardware devices. DFAT is part way through two key initiatives that will deliver a technology refresh across all DFAT systems; namely: the International Communications Network (ICN) Program and the Passport Redevelopment Program. These programs of work will deliver the required technology renewal through several milestones through to June 2018.

1.3.4. *ISM 2015 control 0940*

Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as below extreme risk must be patched or mitigated as soon as possible.

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT systems have a wide global dispersion, servicing 51 partner agencies through domestic and international shared communications infrastructure. DFAT deploys and implements patches categorised below extreme within the shortest possible timeframe.

1.3.5. *ISM 2015 control 0941*

When patches are not available for vulnerabilities, one or more of the following approaches must be implemented:

- *resolve the vulnerability by either: - disabling the functionality associated with the vulnerability - asking the vendor for an alternative method of managing the vulnerability - moving to a different product with a more responsive vendor - engaging a software developer to resolve the vulnerability.*
- *prevent exploitation of the vulnerability by either: - applying external input sanitisation (if an input triggers the exploit) - applying filtering or verification on output (if the exploit relates to an information disclosure) - applying additional access controls that prevent access to the vulnerability - configuring firewall rules to limit access to the vulnerability.*

• *contain exploitation of the vulnerability by either: - applying firewall rules limiting outward traffic that is likely in the event of an exploitation - applying mandatory access control preventing the execution of exploitation code - setting file system permissions preventing exploitation code from being written to disk.*
• *detect exploitation of the vulnerability by either: - deploying an intrusion detection system - monitoring logging alerts - using other mechanisms for the detection of exploits using the known vulnerability.*

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT uses all of the approaches listed depending on the risk imposed by the vulnerability. The primary technical control deployed is an intrusion detection/protection system, which automatically receives feeds that alert and responds to threats. DFAT also manually adds rules to detect specific threats based on ASD advisories. Other elements of the infrastructure also contribute to the security of the system, such as firewalls, File System Permissions.

1.3.6. *ISM 2015 control 1143*

Agencies must develop and implement a patch management strategy covering the patching of vulnerabilities in operating systems, applications, drivers and hardware devices.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT has a mature patch management strategy for Microsoft software products, which will be leveraged to develop an Enterprise Patch Management strategy that covers all technologies used in DFAT by Q1 2016.

1.3.7. *ISM 2015 control 1144*

Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk must be patched or mitigated within two days.

DFAT Compliance status = ***Partially Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT has a procedure in place that aims to meet the two-day patch timeframe. Not all services can be patched within this timeframe due to system limitations; times-zone challenges associated with the DFAT Global ICT reboot cycle; and DFAT and partner agency business imperatives.

Extreme security patches are usually deployed to infrastructure ready for implementation within two days of vendor release. Where systems cannot be patched in two days we have implemented rules on Intrusion Protection Sensor (IPS) to mitigate the vulnerability.

1.4. Restrict administrative privileges

1.4.1. *ISM 2015 control 0445*

Agencies must restrict the use of privileged accounts by ensuring that:

- *the use of privileged accounts are controlled and auditable*
- *system administrators are assigned a dedicated account to be used solely for the performance of their administration tasks*
- *privileged accounts are kept to a minimum*
- *privileged accounts are used for administrative work only*
- *passphrases for privileged accounts are regularly audited to check they meet passphrase selection requirements*
- *passphrases for privileged accounts are regularly audited to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts)*
- *privileges allocated to privileged accounts are regularly reviewed.*

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT manages compliance with the above controls through formal policy and a series of structured processes that ensure privileged accounts are issued, and access maintained on a need-to-hold basis, keeping the number of privileged accounts to a minimum. Privileged accounts are audited to ensure they are only used for administrative purposes; that they meet passphrase complexity requirements; and that passphrases are not reused on the administrator's respective standard account.

1.4.2. *ISM 2015 control 0985*

Agencies must conduct the remote administration of systems, including the use of privileged accounts, over a secure communications medium from secure devices.

DFAT Compliance status = ***Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

DFAT utilise an ASD approved Remote Access System, which incorporates two-factor authentication and encrypted Virtual Private Network (VPN) communications. Administrators are provided departmentally secured laptops to administer DFAT systems remotely.

1.4.3. *ISM 2015 control 1175*

Agencies must prevent users from using privileged accounts to access the Internet and email.

*DFAT Compliance status = **Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

Privileged accounts are prevented from accessing the Internet by membership of a deny group. Privileged accounts are prevented from email access through configuration controls that only allow standard accounts having email access.

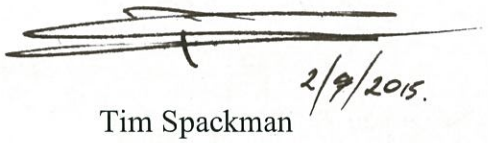
1.4.4. *ISM 2015 control 0405*

Agencies must:

- *limit system access on a need–to–know basis*
- *have any requests for access to a system authorised by the person's manager*
- *provide personnel with the least amount of privileges needed to undertake their duties*
- *review system access and privileges at least annually and when personnel change roles*
- *when reviewing access, ensure a response from the person's manager confirming the need to access the system is still valid, otherwise access will be removed.*

*DFAT Compliance status = **Compliant***
Statement of compliance or detailed plan of necessary activity to achieve compliance:

Access to DFAT ICT systems is only granted upon receipt of an Access Request form, signed by their respective director based on least privilege and Need-to-Know principles. Ongoing access is monitored annually and revalidated with user management.



2/9/2015.

Tim Spackman

Chief Information Security Officer

Department of Foreign Affairs and Trade