IPAC

SECURITY RECOMMENDATIONS FOR UK PARLIAMENTARIANS

October 2023

Table of Contents

CONTENTS

Introduction

INTRODUCTION

In the past three years at least two Security Service Interference Alerts have been issued to Parliament. These highlight the extent to which Westminster is a target for foreign interference. In the wake of another recent scandal regarding alleged interference activities on behalf of the People's Republic of China, some MPs have expressed concern about their capacity to anticipate and defend against suspected foreign interference.

This short paper intends to assess current security apparatus, and offer recommendations to the relevant authorities in line with best practice. Ahead of a General Election, where interference activities are expected to increase, there is an urgent need to increase capacity.

CURRENT SECURITY APPARATUS

A brief overview of current security operations. The following are currently provided to Members:

- **Members' Handbook:**
  - Contains the following security guidance:
    - Requiring Members and staff to wear their pass at all times on the Parliamentary Estate (except when they are being filmed) and take it off when they leave;
    - Remain alert and report any suspicious or unusual incidents to Security Control;
    - Ensuring that desks, filing cabinets and cupboards are kept locked when not in use and that keys are not left in easily accessible places; lock away all private and confidential papers and articles of value;
    - Keeping memory sticks, CDs and other data storage devices in a safe and secure place.
    - Providing guidance to Members and staff to contact the Serjeant at Arms, when they receive malicious or threatening emails[1].

- **Parliamentary email and social media monitoring:** As of 2019, 237 Members have opted into the social media monitoring service[2]. The social media monitoring service allows Members to forward threatening or abusive social media communications to the Police. The scheme does not require police to notify Members of malicious activity, though in practice, this is often what happens. No official record of notifications is held by the House[3].

CURRENT SECURITY APPARATUS

A brief overview of current security operations. The following are currently provided to Members:

- Some members have been referred to the **National Cyber Security Centre (NCSC)**, which provides some services to assist Members, including a take-down service of impersonation accounts. The NCSC will also process suspicious correspondence, and may also report to the police.

- **Parliamentary Pass Vetting:** The Parliamentary Security Department (PSD) is responsible for the security for both Houses. PSD is also responsible for security vetting within Parliament and providing passes. Security clearance is required by everyone working on the Parliamentary estate, requiring access to the Parliamentary network or being given access to sensitive Parliamentary information.

- According to a log of all incidents in House of Commons areas reported to MPS by the Parliamentary Security Department (PSD) between 1 January 2023 and 1 May 2023, 127 incidents were reported, comprising malicious communications, crime or disorder, suspicious activity etc[4].

- Resources: According to data published in 2019, the annual budget for the Members' Security Support Service (MSSS) for 2019-20 was £2.2 million which comprises 10 members of staff [5].

SAFEGUARDING THE BROADER POLITICAL ENVIRONMENT

What needs protection?
(*Paraphrased from Digital Guardian)[6]*

01

Data storage or Data at rest:

Inactive data stored on devices like hard drives, laptops, or external drives. This contrasts with data in transit, which moves between devices or networks. While some might perceive data at rest as less vulnerable, it often becomes a prime target for attackers due to its value. The security of both data at rest and in transit largely depends on the protective measures implemented for each state. Data at rest includes but is not limited to databases, photos, contacts, apps, email and messages stored on smartphones, tablets and computers.

02

Data in transit:

Content of communication, files and information actively moving from one location to another such as across the internet or through a private network. This is data while travelling from network to network or being transferred from a local storage device to a cloud storage device – wherever data is moving. Effective data protection measures for in transit data are critical, as data is often considered less secure while in motion.

03

Data in use:

Data that is currently being processed or consumed by an application or an user. This type of data is not being passively stored, but is instead actively moving through parts of an IT infrastructure. For example, if you are updating a contact list on a spreadsheet, the data in the list are "in use" while it is opened and edited.

SAFEGUARDING THE BROADER POLITICAL ENVIRONMENT

What needs protection?
(*Paraphrased from Digital Guardian*)

04

Physical security [7]:

Tangible assets, information, personnel. These require protection against unauthorised physical access, harm, or theft. It encompasses a range of preventive and responsive actions designed to deter, delay, detect, and respond to potential threats. It includes the protection of sensitive documents, electronic devices, staff and personnel, meeting spaces, communication infrastructure and physical assets. In the Parliamentary context, this category should also be understood to cover activity which may compromise the integrity of the Parliamentary process.

"

> It is important to emphasise that security risks are different for every person, due to behavioural variations. Members and their staff do not use technology, or undertake their parliamentary operations in exactly the same way. Comprehensive risk modelling should be bespoke and take into account variations in working style. That said, there are general steps that can be taken to raise the level of security of Westminster.

RECOMMENDATIONS

Capacity Building	**Risk Assessment**	**Remedial**
Announce **mandatory and regular** training on digital and operational security for Members of the Houses and their staffers, and provide follow-ups and troubleshooting channels. Disclose the names of Members who fail to complete the training.	Conducting **comprehensive audit** annually, including analysis of threats and analysis of vulnerabilities; with a view to deriving up-to-date counter measures to protect the parliamentarians and their staff	**MSSS should be afforded sufficient resources** to monitor and notify parliamentarians and staffers immediately when they detect an attack and provide suggested remedies, and to expand security support more generally.
Provide access to basic tools like trustworthy VPNs, physical authenticators, faraday bags, password managers, privacy screen protectors etc.	**Issue audit checklist** for members and encourage them to conduct regular audits of their own offices [8]	**Create Parliamentary incident report mechanism** allowing Members and staff to report attacks, stolen devices, data breaches etc.
Send regular warning emails about new possible types of attack, phishing, mobile malware, malicious applications	**MSSS to consider providing enhanced security support** to Members of both Houses and their staff who are judged to be more exposed to security threats.	Prepare **crisis response guidance** for Members, signposting recommended actions in the event of major incidents, such as hacking, theft etc, and including guidance on how to deal with threatening or suspicious individuals or groups.

RECOMMENDATIONS

Capacity Building

Develop comprehensive security handbook for Members and staff [9], incorporating at the least:

- Regularly updated digital security checklists [10]
- Information on：
    - password management
    - Social media management
    - Multi factor authentication, encryption, secure hardware, safe browsing and secure deletion of data
    - Assistance in identifying ‘critical information’ that requires enhanced protection.
    - Security onboarding and offboarding policies for staff
- Guidance for Members and staff on handling external visitors, covering security protocol, due diligence, and operational security on site.
- Travel advice with regards to physical and digital security [11]

MSSS to consider ‘mystery shopper’ security tests, for example, phishing exercises to test Members and staff’s ability to recognise and respond to a phishing attack [12]

Create an anti-interference and security handbook for dissemination among parliamentary candidates. [13]

Parliamentary authorities should consider **strengthening access controls** to the Estate:

Implement ID checks for all visitors, deny admittance to Westminster offices without invitation, limit staff escort privileges to those with a confirmed invitation[14] [15].

Footnotes

FOOTNOTES

[1] UK Parliament Members' Handbook

[2] Numbers published by the authorities under FOIs

[3] Answer given by the UK Parliament Authorities in a Freedom of Information release.

[4] Answer given by the UK Parliament Authorities in a Freedom of Information release.

[5] Figures published by UK Authorities in 2019.

[6] https://www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

[7]https://www.techtarget.com/searchsecurity/feature/Best-practices-to-secure-data-at-rest-in-use-and-in-motion

[8] Safetag provides a very comprehensive auditing model that is adaptive to the size of organisations

[9] New Zealand has issued Security Advice for Members of the New Zealand Parliament and Locally Elected Representatives and a guide to help mitigate the risks associated with Foreign Interference.

[10] The Ford Foundation has created a Cybersecurity Assessment Tool in the form of a questionnaire to provide adaptive suggestions to organisations and institutions.

[11] New Zealand has issued travel advice for government officials travelling overseas on business.

[12]Audrey Tang, the Minister of Digital Affairs in Taiwan has conducted phishing drills with officials.

[13] The Belfer Center at Harvard, the International Republican Institute and the National Democratic Institute have created a security campaign playbook for political campaigns.

[14]The Northern Ireland Assembly offers a regulation for visitors and set out the general rules of entry for visitor:

[15] The US's regulations and Prohibition list on Capitol Hill.

IPAC SECURITY RECOMMENDATIONS

This report is sent to the Speakers of both Houses of Parliament in the UK with recommendations for improving the security of Parliamentarians.

CONTACT

Inter-Parliamentary
Alliance on China

www.ipac.global
info@ipac.global
@ipacglobal