GREATER**LONDON**AUTHORITY

REQUEST FOR ASSISTANT DIRECTOR DECISION –ADD2565

Title: NRMM LEZ website security review and update

Executive summary:

In 2015 the Non-Road Mobile Machinery Low-Emission Zone (NRMM LEZ) was established using the Mayor's strategic planning powers. To facilitate the successful delivery of the programme a website was developed to enable the construction industry to register NRMM used in London and to demonstrate compliance.

Security issues have been identified in the live website. It is recommended that a review of website security is undertaken; and data production and service delivery threats are fixed through new secure coding approaches.

To identify and address these security threats, Assistant Director approval is sought to approve the spend of £50,000. This spend will be split between financial years 2021-22 and 2022-23 with spend of £30,000 and £20,000 respectively.

Decision:

That the Assistant Director of Environment and Energy approves:

1. the spend of £50,000 to identify and address security threats on the NRMM LEZ website
2. an exemption from the requirements of the Contracts and Funding Code, to enable the procurement of the services mentioned in decision 1 under the GLA's existing call-off contract with Sirius dated 10 August 2020.

AUTHORISING ASSISTANT DIRECTOR/HEAD OF UNIT

I have reviewed the request and am satisfied it is correct and consistent with the Mayor's plans and priorities.

It has my approval.

Name: Catherine Barber	**Position:** Assistant Director, Environment and Energy
Signature: 	**Date:** **14/3/22**

PART I – NON-CONFIDENTIAL FACTS AND ADVICE

Decision required – supporting report

1. Introduction and background

1.1. In 2015, the Mayor established a Non-Road Mobile Machinery Low-Emission Zone (NRMM LEZ) using his strategic planning powers. To facilitate the successful delivery of the programme a website was developed to enable the construction industry to register NRMM used in London, and to demonstrate compliance. The website is also the tool for the GLA to issue exemptions and to audit site compliance.

1.2. The NRMM LEZ website forms part of the GLA Digital Estate.

1.3. In 2021, Sirius, the GLA Digital Estate Support Partner, was instructed to develop new functionality on the existing NRMM website, to enable GLA Group NRMM to be logged in the system. This was approved through MD2813. During this website development, Sirius identified security threats within the code of the existing live website. These security issues fall outside of the scope of the new functionality development. Work is required for the NRMM website to address these identified security threats.

1.4. Additional work is also required to complete a full security review of the NRMM website to identify and address further security vulnerabilities. The cost of this work is dependent on the number of security issues that are identified and the complexity of the solution. We anticipate it to be £50,000, based on the assumption of eight weeks' work. The work will be undertaken by the GLA Digital Estate Support Partner.

2. Objectives and expected outcomes

2.1. The objective of this decision is to address the security vulnerabilities within the NRMM LEZ website. By enabling this work, the GLA will be able to better protect data contained within the NRMM website and reduce the risk of website security threats. This outcome will enable the NRMM LEZ policy to continue to be delivered in London.

2.2. This ADD seeks budget approval to deliver the NRMM website security review. The work will be delivered under an existing call-off contract, approved in MD2590.

<u>Procurement of the services</u>

2.3. In 2020 approval was granted under MD2590 to appoint a call-off support and maintenance contract covering the entire GLA Digital Estate. The NRMM LEZ website falls within the scope of the GLA Digital Estate.

2.4. The GLA procured Sirius via a call-off under the G-Cloud framework agreement. The G-Cloud framework is a public sector gov.uk digital marketplace procurement platform. The process of onboarding suppliers onto GCloud is not owned by the GLA; however, all digital marketplace frameworks and CCS frameworks can be used by all public sector organisations to procure items and services. Only one supplier, Sirius, met the scope requirements for the support and maintenance contract. Following the conclusion of the procurement process, the GLA entered into

a call-off contract with Sirius dated 10 August 2020. The total value of the call-off contract was up to £750,000.

2.5. The call-off contract scope includes the entire GLA digital estate. Schedule 1 (Services) of the contract 'R13 – Projects' states: "The Supplier may be required to provide Agile development team resources to develop new digital products or carry out major changes to an existing product or service". Sirius is the only development supplier that is contracted to GLA's Technology Group for product development work, and is able to develop in the technology on which NRMM is built. No contract variation is required.

2.6. An exemption from section 9 of the Authority's Contracts and Funding Code (the Code) is required for this security work, on the basis of section 10 of the Code. This is justified because the services comprise the continuation of existing work that cannot be separated from the new work. Sirius currently provides support and maintenance of the NRMM website via the support and maintenance contract. Additionally, Sirius is in the process of developing an update to the NRMM, as approved in MD2813. It was during this website development that the security issues were identified. These security issues are a continuation of this workstream, and cannot be separated from it. Furthermore, the continued use of Sirius provides the GLA value for money, as a new supplier would require additional preparation work to be able to work on the project.

2.7. The development work will be charged on a time and materials basis, as set out in the GLA digital estate call-off contract.

3. Equality comments

3.1. The GLA and other public authorities must have 'due regard' to the need to eliminate unlawful discrimination, harassment and victimisation; and to the need to advance equality of opportunity, and foster good relations, between people who share a protected characteristic and those who do not, under section 149 of the Equality Act 2010. This involves having due regard to the need to remove or minimise any disadvantage suffered by those who share a relevant protected characteristic; taking steps to meet the different needs of such people; and encouraging them to participate in public life or in any other activity where their participation is disproportionately low.

3.2. The "protected" characteristics and groups are: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage/civil partnership status. Compliance with the Equality Act may involve treating people with a protected characteristic more favourably than those without one. The duty must be exercised with an open mind and at the time a decision is taken in the exercise of the GLA's functions. Conscientious regard must be had that is appropriate in all of the circumstances.

3.3. In January 2019 the GLA published analysis on exposure to air pollution. This showed not only that there are huge health impacts of pollution, but also that these fall disproportionately on the most vulnerable, more deprived people; and Black, Asian and Minority Ethnic communities. This means that improving air quality is fundamentally about tackling social injustice and health inequalities.

3.4. The report considered pollution exposure in London and how exposure varies by age, indicators of relative deprivation and ethnic group. It also looks at total exposure (broken down by borough) and exposure at schools. Through this research, the GLA sought to understand inequalities in

access to clean air in London and consider how this will be improved by planned air pollution controls.

3.5. The research showed that, on average, the most deprived 10 per cent of the population is exposed to concentrations of NO2 that are 25 per cent higher than the least deprived 10 per cent of the population. It is important to note that hidden within this are pockets of extreme wealth with very high levels of exposure, e.g. those living in parts of Westminster, and the Royal Borough of Kensington and Chelsea.

3.6. In terms of ethnicity, research has found there are on average higher concentrations of NO2 in areas that have higher percentages of non-White ethnic groups, with a particularly skewed distribution for the Black/African/Caribbean/Black British population. A greater proportion of mixed, Black and other ethnic groups are exposed to levels of pollution that exceed the NO2 limit value than their proportion of the total population.

3.7. The work set out in this ADD enables the continuation of the delivery of the NRMM LEZ. This will benefit all Londoners, but due to the unequal impacts of pollution on the most vulnerable Londoners there is likely to be a positive effect in tackling social and health inequality of this programme of activity.

4. Other considerations

Risks and issues

4.1. Without immediate action being taken, the NRMM website is at risk of a malicious attacker retrieving, updating or amending data in the NRMM database. A full security review is advised. Not taking action is not considered a viable option.

4.2. An alternative solution considered is to build a new NRMM website. This option would be more expensive than the proposed security review and is not advised.

4.3. An interim solution has been taken to move key functions to Citrix access only, limiting access to GLA employees only. This is not a long-term solution, as it does not address all identified issues and limits website functionality. A full security review is required to identify further security issues subsequently a code change and website update is required.

Issue	Impact	Likelihood	Severity	Mitigation
Missing authorisation checks on back-end endpoints (e.g. the server, the database, scripts)	A malicious attacker could register as a user, and then submit requests to amend or delete data for organisations to which they do not belong.	Limited coding knowledge, and a basic level of hacking experience, are required. A single line of code could be used to achieve this.	Very high	Extensive development work.
Query injection	This would enable any SQL code to be executed on the back-end.	Advanced hacking skills may be required. If the vulnerability is found, then exploiting the	High	Rewrite appropriate queries to prevent SQL injections.

	Attackers could potentially retrieve, update or amend data in the database.	attack is straightforward.		
Exposure of users' password data	Password data could be decoded and used to gain unauthorised access to organisations and user data in the system.	Some coding knowledge, and a basic level of hacking experience, are required. A single line of code could be used to achieve this.	Medium	Error-handling on the site needs improvement.

4.4. Delays in undertaking any of the activities listed are likely to lead to an interruption in service provision and a security breach that may have a negative reputational impact.

4.5. Due to the size of the security issue being uncertain until a security review takes place, the cost of the solution is uncertain. A further DD will be produced if expenditure is likely to exceed greater than 10 per cent of the value requested in this ADD.

Links to Mayoral strategies and priorities

4.6. The actions proposed above will contribute to delivering Proposal 4.2.3.a in the London Environment Strategy: the Mayor will work with government, TfL, the London boroughs, the construction industry and other users of NRMM, such as event organisers, to prevent or reduce NRMM emissions.

Consultations and impact assessments, including data protection

4.7. The GLA has a responsibility under GDPR to protect personal data. The security review is fundamental to ensure GDPR compliance remains.

4.8. Very limited personal data under GDPR is held on the NRMM website and associated database. The data is likely to be of low value to potential website hackers.

4.9. The GLA DevOps team is currently undertaking a review of the data logs to identify possible breaches. These data logs will continue to be reviewed regularly going forward until the security review has been completed.

Conflicts of interest

4.10. There are no conflicts of interest to note for any of those involved in the drafting or clearance of the decision.

5. Financial comments

5.1. Expenditure of up to £50,000 is required to review security for the NRMM LEZ website and resolve any threats to data and service delivery. The precise cost of this work is dependent upon the number of security issues identified and the complexity of the solution.

5.2. As the NRMM LEZ website forms part of the Authority's Digital Estate, the required maintenance work will be undertaken by the current digital support partner.

5.3. The budget provision for this work will come from the Air Quality programme held within the Environment Unit. The sum of £30,000 will be funded from 2021-22 underspends, whilst the £20,000 balance has been included in the 2022-23 indicative budget proposals – the latter of which is still subject to approval.

6. Legal comments

6.1. The foregoing sections of this report indicate that the decisions requested of the assistant director fall within the statutory powers of the Authority to promote and/or to do anything that is facilitative of or conducive or incidental to the improvement of the environment within Greater London and in formulating the proposals in respect of which a decision is sought officers have complied with the Authority's related statutory duties to:

- pay due regard to the principle that there should be equality of opportunity for all people
- consider how the proposals will promote the improvement of health of persons, health inequalities between persons and to contribute towards the achievement of sustainable development in the United Kingdom
- consult with appropriate bodies.

6.2. In taking the decisions requested of her, the assistant director must have due regard to the Public Sector Equality Duty – namely the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between persons who share a relevant protected characteristic (race, disability, age, sex, sexual orientation, religion or belief, pregnancy and maternity, and gender reassignment) and persons who do not share it; and to foster good relations between persons who share a relevant protected characteristic and persons who do not share it (section 149 of the Equality Act 2010). To this end, the assistant director should have particular regard to section 3 (above) of this report.

6.3. The procurement of the services from Sirius is valued at up to £50,000. Section 9 of the Authority's Contracts and Funding Code (the Code) requires that the Authority undertake a formal tender process or make a call off from an accessible framework agreement for procurements with a value between £10,000 and £150,000. However, section 10 of the Code also provides that an exemption from this requirement may be justified on the basis that the services comprise the continuation of existing work that cannot be separated from the new work. The officers have set out at paragraphs 2.3 to 2.7, above the reasons that the procurement of Sirius falls within the said exemption. Accordingly, the Assistant Director may approve the exemption, if she be so minded.

7. Planned delivery approach and next steps

Activity	Timeline
Identification of urgent security threats in admin page	March 2022
Code fix and deployment of solutions	March 2022
Wider security review of NRMM website	April 2022
Code fix and deployment of solutions	April 2022

Appendices and supporting papers: None

Public access to information

Information in this form (Part 1) is subject to the Freedom of Information Act 2000 (FoIA) and will be made available on the GLA website within one working day of approval.

If immediate publication risks compromising the implementation of the decision (for example, to complete a procurement process), it can be deferred until a specific date. Deferral periods should be kept to the shortest length strictly necessary. **Note**: This form (Part 1) will either be published within one working day after it has been approved or on the defer date.

Part 1 – Deferral

Is the publication of Part 1 of this approval to be deferred? YES

If YES, for what reason: This ADD highlights potential security vulnerabilities with the live NRMM LEZ website. These vulnerabilities should not be published until the risks have been resolved.

Until what date: 31 July 2022

Part 2 – Sensitive information

Only the facts or advice that would be exempt from disclosure under the FoIA should be included in the separate Part 2 form, together with the legal rationale for non-publication.

Is there a part 2 form –NO

ORIGINATING OFFICER DECLARATION:	Drafting officer to confirm the following (✓)
Drafting officer: Sarah Morris has drafted this report in accordance with GLA procedures and confirms the following:	✓
Corporate Investment Board This decision was agreed by the Corporate Investment Board on 14 March 2022.	✓

ASSISTANT DIRECTOR OF FINANCE AND GOVERNANCE:

I confirm that financial and legal implications have been appropriately considered in the preparation of this report.

Signature **Date**

Anna Custodi **14/3/22**