ACTION HISTORY OF RTI REQUEST No.FSOID/R/E/23/00092

Applicant Name	Sunny Roy K C
Text of Application	The website fsi.nic.in has not been functioning at least since 15th August 2023. In a response received from NIC on the same, it has been notified that fsi.nic.in has been the victim of a defacing attack and also notified by CERT-In. Please see the supporting document. Based on the recommendation of NIC, please provide information for the following questions: 1) Has FSI requested for an audit of fsi.nic.in through a Cert-In empanelled auditor/agency after it was notified by CERT-In that the website may possibly be a victim of defacement attack? 2) If yes, provide the date during which the request was made and the name of the auditor/agency that is conducting the security audit. 3) If no such audit was requested by FSI, may you please let me know why? 4) Is there a tentative date by by which FSI plans to conduct the security audit and notify NIC regarding the audit? Thank you very much for your cooperation in this regard.
Reply of Application	please find attachment for sought information.

SN.	Action Taken	Date of Action	Action Taken By	Remarks
1	RTI REQUEST RECEIVED	20/10/2023	Nodal Officer	
2	REQUEST FORWARDED TO CPIO	23/10/2023	Nodal Officer	Forwarded to CPIO(s) : (1) Kamal Pandey
3	REQUEST DISPOSED OF	10/11/2023	Kamal Pandey-(CPIO)	

Print

1. What does ONHOLD category on Zone-H mean?

   Zone-H is a publicly available archive/repository for defaced websites, sometimes, the hackers themselves submit their hacked pages to this archive. The defacing incidents are maintained under ON HOLD category by Zone-H pending confirmation of defacement.

2. Is the website a victim of a defacement attack?

   Yes, notification in this regard was also received from CERT-In.

3. If the answer to the above question is YES, then what security lapses may have led to the defacement attack?

   Website fsi.nic.in is developed, maintained and hosted by FSI and is hosted at FSI data Centre. Some of the reasons for defacement attack can be vulnerable website code, improper configuration at web server level, unpatched/outdated web server, weak passwords etc. However, exact reason for the defacement can be identified by analysing relevant artefacts.

4. What is to be done by FSI and NIC, to bring the website live again?

   FSI/Owner organisation has to get the website audited through CERT-In empanelled auditor/agency and should submit the website audit certificate and report to NIC to get the website unblocked.

संख्या.22–284 / 2023–एफ0जी0डी0 2798

भारतीय वन सर्वेक्षण

पर्यावरण, वन एवं जलवायु परिवर्तन मंत्रालय

भारत सरकार

कौलागढ़ रोड़, पी0ओ0 – आई0पी0ई0

देहरादून– 248195

दिनांक: 02 नवम्बर, 2023

सेवा में,

लोक सूचना अधिकारी
भारतीय वन सर्वेक्षण
कौलागढ़ रोड़, देहरादून।

विषयः– RTI Application under Right to information Act, 2005.

संदर्भः– आपके पत्र संख्याः 13–6 / 2023–आर.टी.आई–2780 दिनांक 31 अक्टूबर, 2023

महोदय,

उपरोक्त विषय के संदर्भ में सूचित किया जाता है कि Shri Sunny Roy K C की RTI आवेदन संख्या FSOID/R/E/23/00092 दिनांक 20.10.2023 के क्रम में माँगी गयी सूचनायें निम्न है।

S. No	Question	Answer
1	Has FSI requested for an audit of fsi.nic.in through a Cert-In empaneled auditor /agency after it was notified by CERT-In that the website may possible be a victim of defacement attack?	Yes
2	If, yes provide the date during which the request was made and the name of the auditor/agency that is conducting the security audit.	Date:28th August,2023 Name of Agency:(M/sMaverick Quality Advisory Services Pvt Ltd, 123 Radhey Shyam Park, P.O Sahibabad, Ghaziabad, Uttar Pradesh-201005
3	If no such audit was requested by FSI, may you please let me know why?	Not Applicable
4	Is there a tentative date by which FSI plans to conduct the security audit and notify NIC regarding the audit?	Security audit completed and certificate has been issued on date 13.10.2023 & informed NIC regarding security audit certificate on date 13.10.2023

भवदीया,

02/11

RTI (04

1/11/23

(मीरा अय्यर)
भा.व.से.
संयुक्त निदेशक (एफ.जी.डी.)