W-43/11/2021-IPHW
Government of India
Ministry of Electronics and Information Technology
(IPHW Division)

Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi-110003.

Dated: 11 Mar, 2024

OFFICE MEMORANDUM

Subject: -Advisory on the Threat of Information Leakage through CCTV/ Video Surveillance system (VSS)/ Digital Video Recorders /Network Video Recorders-reg

The reference is made to the concerns raised by various Ministries/Departments regarding the security implications associated with the deployment of Closed-Circuit Television (CCTV) Cameras and the conduct of cyber auditing and testing of hardware pertaining to CCTV cameras and other Internet of Things (IoT) devices. The Ministry of Electronics and Information Technology (MeitY) has formulated comprehensive security guidelines for CCTV cameras as included in **Annexure 'A'**.

2. In light of these concerns, Government Ministries/Departments are strongly advised to adhere to the guidelines outlined within the ambit of the Public Procurement Orders to safeguard the overall security and integrity of CCTV Cameras and IoT Devices.

3. This issues with the approval of the Competent Authority.

(Asha Nangia)

Group Coordinator & Scientist-'G'
Ph. 011-24301965

To,

i) Secretaries of All Ministries/Department of Government of India

ii) Chief Secretaries/Administrators of Union Territories/National Capital Territory of Delhi

Annexture- 'A'

A video surveillance system, also known as Closed-Circuit Television (CCTV) system, is a collection of cameras and other related equipment used to monitor and record activities in a specific area commonly used for security and surveillance purposes.

2. Key components of a video surveillance system typically include cameras, (Analog, Digital, IP Cameras), Video Management System (VMS) Software, Storage (Network Video Recorders (NVRs) or Digital Video Recorders (DVRs)), Power Supply etc.

3. While these surveillance technologies undoubtedly offer a range of benefits and are valuable tools for monitoring and security, they also raise certain concerns and risks. Some of the growing risks associated with CCTV systems include data security, privacy breach, hacking and cyber-attack etc. Various incidents have also been reported due to security flaw in the surveillance cameras.

4. The cybersecurity is an ongoing process, so staying vigilant and keeping system up to date with the latest security practices can significantly enhance the security of CCTV system and protect it from potential threats and unauthorized access. In this regard, the following measures are advised to minimize the risk associated with CCTV surveillance system:

i) The Rules and regulations as applicable, notified by the Government or procurement of goods and services must be followed e.g.
    a) Public procurement Order (Make in India), 2017
    b) Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021

ii) BIS has formulated Blank Detail Specification (BDS) for IS 16910 for performance requirements of CCTVs. The procuring government agency can stipulate their own technical requirements for the parameters listed in the BDS and the testing can be done as per the test methods prescribed in the standard.

iii) The procurement of Video Surveillance System from the brand having history of security breaches and data leakages should be avoided.

iv) **Hardware Security**: For the Hardware Security testing of CCTV cameras, the government agencies should use the testing infrastructure available with Standardization Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time for testing the CCTVs as per the Essential Requirement(s) notified under the PPO for CCTV.

v) **Network Security**: The general cyber security practices for installation and monitoring should be also be adopted. Maintain the network isolation (Air-Gap) from the public network to minimize the risk of unauthorized access and potential cyberattacks. Wherever, air gap is not possible, Network segmentation, secure tunnel/Virtual Private Network (VPN) /Dedicated Lease Line etc. should be used for restricting access to CCTV systems and isolate them from critical infrastructure and sensitive data. Use MAC address binding to prevent the unauthorized access by unidentified devices.

vi) **Secure Physical Access:** Restrict physical access to the CCTV control room and equipment. Only authorized personnel should have access to the system. Use locks, access control systems, and surveillance measures to protect the equipment.

vii) **Strong Passwords:** Change default passwords immediately upon installation and use strong, unique passwords for all cameras, recorders, and access points. Avoid using easily guessable information or common words.

viii) **Regular Firmware Updates:** Manufacturers often release updates that address security vulnerabilities. Regularly check for updates and apply them promptly keeps the firmware and software of your CCTV devices up to date.

ix) **Encryption of Data:** Ensure all communication between cameras, recorders, and viewing devices is encrypted. This prevents unauthorized individuals from intercepting and accessing sensitive information.

x) **Disable Unused Features:** Turn off or disable any features and services that are not necessary for the proper functioning of the CCTV system. Each enabled feature potentially introduces another security vulnerability.

xi) **Secure Remote Access:** If remote access is required for maintenance or monitoring, implement a secure VPN (Virtual Private Network) for remote connections. Avoid exposing the system directly to the internet whenever possible. IPBEUs (IP-Based Encryption Unit) to safeguard data transmission between cameras and recording devices, Lease Line for dedicated and secure

network connectivity and Implementation of data diodes to ensure unidirectional flow of information, enhancing security.

xii) **Regular Auditing and Monitoring:** Monitor the CCTV system logs for unusual activities and potential security breaches. Regularly audit the system to ensure that everything is functioning correctly and there are no unauthorized access attempts.

xiii) **Physical Camera Security:** Position cameras in a way that prevents tampering and vandalism. Use vandal-resistant camera housings and install them in high and secure locations where they are less likely to be tampered with.

xiv) **User Access Control:** Implement a strict access control policy to limit the number of individuals who can access the CCTV system and its data. Assign different levels of access based on roles and responsibilities.

xv) **Data Storage and Retention:** Ensure proper data storage and retention policies are in place. Securely store recordings and define how long data should be retained before it gets automatically deleted. Data Storage should be in terms of storage duration (number of Days) based on operational requirements rather than storage capacity. The data storage of all CCTVs installed at Government Establishment/Public Places should be mandated to be within the India even if it is stored in cloud platforms.

xvi) **Staff Training:** Provide comprehensive training to employees and system administrators on security best practices. Make sure they understand the potential risks and how to mitigate them effectively.

xvii) **Regular Security Assessments:** Conduct periodic security assessments and penetration tests to identify vulnerabilities and weaknesses in the CCTV system. Address any issues discovered promptly.

xviii) **Tender/RFP** should encompass both Hardware and Software parts of the Bill of Materials (BoM) combined presenting comprehensive specifications for these components to facilitate the interoperability of the HW/SW as a whole in the VSs system. Model Technical Specifications/Guidelines for CCTVs/VSS issued by MHA from time to time, should be adopted while formulating the technical specifications for procurement of CCTV/VSS.

xix) **CCTV Device testing and certification:** CCTV Cameras (Analog/ IP/ Analog Speed Dome/ IP Speed Dome) should comply with the Essential Requirements (ERs) notified as part of the PPO for CCTV in Gazatte of India (EXTRAORDINARY, PART II—Section 3—Sub-section (ii) dated 7th March,

2024, at Sr. No. No. 1062) to ensure the security of the VSS / CCTV systems, as amended from time to time. The security testing certificate for CCTV/VSS to be issued by Standardisation Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time. The validity of the test report issued by STQC Lab will be three years from the date of issue of the report.

5. In this regard, the Government Ministries, Departments are advised to instruct the Chief Information Security Officers (CISOs) of their respective organizations and subordinate organizations for enforcing the above measures to address the security threats of the CCTV network vulnerability and to ensure the overall security and integrity of CCTV/Video Surveillance Systems.

======**********======