

Agenda Item 5

Strategy and Resources Committee 24/07/2024 – Written responses to Public Questions

1. Questions from Adi Li

Question: Following my second email inquiry to the FOI on 3 June asking about the names of manufacturers of CCTV and where the CCTV are made which are used in public and government buildings as well as the public question I asked last Wednesday 17 July at the Sheffield council meeting regarding the concerns about potential cybersecurity threats associated with CCTV being used in public and government buildings in Sheffield. One of the main concerns is the creation of backdoor channels by Chinese manufacturers to the Chinese government to remotely access data, and I am going to follow up on the CCTV issue at this Strategic and Resource Policy Committee meeting.

Firstly, I would like to thank Councillor Tom Hunt for his positive response at the Sheffield Council meeting where he stated that one of the considerations was the replacement of existing CCTV at the end of the product's life. However, waiting for the end of a product's life cycle can take years or even ten years, and the challenges are imminent.

I would like to share some information that may assist in identifying potentially effective ways to deal with CCTV issues, and I look forward to hearing from your committee on specific timelines and implementation plans.

If you look inside a CCTV, there is an NVR (network video recorder) that records the video data transmitted from the CCTV and stores it in a format that can be accessed later. The function of NVR is to transmit data and images, and can access data and monitor terminals through the network.

An optimistic approach would be to replace all CCTV within a timetable to ensure there is no risk.

Due to financial considerations, can I ask Sheffield Council to look into ways to replace the NVR? The captured images and data remain in the CCTV, but changing the NVR can cut off data transmission or uploading or downloading activities by unauthorised parties.

Can we try to source NVRs from local suppliers or other countries to address the potential risks posed by products associated with the Chinese government?

Response: Sheffield City Council is conducting a review of CCTV across all council sites. Where Hikvision NVR's and cameras are in use and connected to an internet facing network, an asset replacement program will be undertaken to replace all Hikvision NVR's and to update all Hikvision cameras with new firmware and security credentials so that it will not be possible to connect through to any internet or network connection for remote access. As a council we have already implemented this at the Botanical Gardens.

All replacement NVR's will be of non-Chinese origin and, as an added security measure, all will have complex passwords enforced, have stringent cyber security credentials and be NDAA (National Defence Authorisation Act) compliant.

With regards to the likely timescales for this work, we are currently engaged in a tender process to procure a new CCTV contractor. Once the contractor commences,

we will be embarking on a 5-year maintenance and replacement program. During this period, all cameras will be switched over to IP (Internet Protocol) cameras and this work will include replacement of Hikvision cameras.

Answers to all other public questions were provided at the meeting and details are available in the minutes and in the webcast here: [Agenda for Strategy and Resources Policy Committee on Wednesday 24 July 2024, 2.00 pm | Sheffield City Council](#)