



भारत सरकार Government of India
रेल मंत्रालय Ministry of Railways
रेलवे बोर्ड (Railway Board)



No.2024/TeleDev/Security in CCTVSystem(3454081)

Dated:18.03.2024

General Manager
Zonal Railways,
Production Units

Director General
RDSO
Lucknow

Director General
Centralized Training Institutes

Sub.: Implementation of Gazette Notification and advisory on CCTV cameras and software
Ref: (i)MeitY, Gol – Gazette Notification No CG-DL-E-08032024-252738 dtd 07.03.2024
(ii)MeitY, Gol – w43/11/2021-IPHW dtd 11.03.2024

MeitY, vide its Gazette Notification at reference (i) above, has notified electronic products of Video Surveillance System under the Public Procurement(Preference to Make in India) Order 2017) and Essential Requirement(s) for Security of CCTV. (Attached as Annexure-I)

MeitY, vide its OM at reference (ii) above has also issued advisory on the Threat of information leakage through CCTV/ Video Surveillance System (VSS)/ Digital Video Recorders /Network video Recorder.(Attached as Annexure-II)

In addition to above, STQC has been engaged with the approval by Member (Infra) to undertake activities for cyber security of CCTV System for which budgetary quotation has also been obtained from STQC (Attached as Annexure-III).

Since the matter is concerned with security of entire Video Surveillance System (VSS) network of IR, following directives are issued for immediate implementation:

RDSO, RCIL, CRIS, Zonal Railways, Production Units and Centralized Training Institutes (CTIs) are advised to comply with the above notifications of MeitY, Gol. For compliance of above directives, in case any changes are required in RDSO VSS specifications/Tender Conditions, same may be done with immediate effect.

This issues with the approval of Additional Member (Tele).

DA: As mentioned above

रणजीत
18-3-2024
(रणजीत कुमार)
कार्यकारीनिदेशक(दूरसंचारविकास)
रेलमंत्रालय
011-47843012, edtd@rb.railnet.gov.in

Copy to CMD/RCIL, MD/CRISfor information and necessary action pl.

		और विकास प्रक्रियाओं के हिस्से के रूप में एक या अधिक अद्यतन मैलवेयर पहचान उपकरण नियोजित किए जाएंगे। अंतिम पैकेजिंग और प्रदायगी से पहले मैलवेयर पहचान तकनीकों का उपयोग किया जाएगा (उदाहरण के लिए, एक या अधिक अद्यतन मैलवेयर पहचान उपकरणों का उपयोग करके मैलवेयर के लिए तैयार उत्पादों और घटकों को स्कैन करना)।	पहचान टैनिंग/जालसाजी, सीएम टूल के ट्रेकिंग लक्ष्यों की आवश्यकता के रूप में की गई है। गुणवत्ता आश्वासन प्रक्रिया को प्रस्तुत करने और उसे प्रदर्शित करने की आवश्यकता है।	
		4.4 आपूर्ति श्रृंखला जोखिम की पहचान, मूल्यांकन, प्राथमिकता और शमन आयोजित किया जाएगा।		आपूर्ति श्रृंखला जोखिम / व्यापार निरंतरता योजना नीति दस्तावेज, प्लेबुक जो दर्शाती है कि आपूर्ति श्रृंखला व्यवधान को कैसे संभालना है, घटना के बाद सारांश दस्तावेजों को प्रस्तुत करने और उसी को प्रदर्शित करने की आवश्यकता है।

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(IPHW DIVISION)

NOTIFICATION

New Delhi, the: 6th March, 2024

Subject: Public Procurement (Preference to Make in India) Order 2017-Notifying CCTV/ Video Surveillance System for Security in furtherance of the Order

Reference:

(i) Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P-45021/2/2017-B.E.-II dated 15.06.2017, as amended by Orders dated 28.05.2018, 29.05.2019, 04.06.2020 and 16.09.2020

(ii) Ministry of Electronics and Information Technology (MeitY) Electronic Products Notification No. W-43/4/2019-IPHW-MeitY dated 07.09.2020

S.O. 1119(E).—The Government has issued Public Procurement (Preference to Make in India) Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 15.06.2017, as amended by Orders dated 28.05.2018, 29.05.2019, 04.06.2020 and 16.09.2020, to encourage 'Make in India' and promote manufacturing and production of goods and services in India with a view to enhancing income and employment.

2. In furtherance of the Public Procurement (Preference to Make in India) Order 2017 [PPP-MII Order 2017] notified vide reference cited above, the Ministry of Electronics and Information Technology (MeitY) hereby notifies

that preference shall be provided by all procuring entities to locally manufactured Video Surveillance System for Security as per the aforesaid Order, as amended from time to time.

3. For the purpose of this notification:

3.1 The definition of Class-I local supplier, Class-II local supplier and Non-local supplier shall be as per paragraph 2 of the DPIIT PPP-MII Order 2017 No. P-45021/2/2017-PP(BE-II) dated 16.09.2020, as amended from time to time. The mechanism for calculation of local content is prescribed for each notified Electronic Product in this notification.

3.2 Paragraph 3A of the DPIIT PPP-MII Order 2017 No. P-45021/2/2017-PP(BE-II) dated 16.09.2020, as amended from time to time, shall be referred for percentage of procurement for which preference to domestically manufactured Electronic Products is to be provided (in value terms).

4. Following electronic products of Video Surveillance System are notified under the Public Procurement (Preference to Make in India) Order 2017:

4.1 Video Surveillance System

Definition:

For the purpose of this Notification, Video Surveillance System is usually a system that *inter-alia* includes: (i) Closed Circuit Television (CCTV) Camera (Analog/ IP/ Analog Speed Dome/ IP Speed Dome), (ii) Digital Video Recorder (DVR) / Network Video Recorder (NVR). Some of the applications of Security and Video Surveillance System are surveillance of Cities, Schools, Banks, Government Offices, public places, traffic monitoring and home security, etc.

4.2 Mechanism for calculation of local content of CCTV Camera (Analog):

The domestic BOM of CCTV Camera (Analog) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (Analog)	Value addition / local content required for the input to be classified as domestic BOM		
	(1)	(2)		
1.0	Main PCB*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BOM of the CCTV Camera (Analog)		
(i)	I/O Board (optional)			
(ii)	Infrared (IR) Board (optional)			
(iii)	Control Board (optional)			
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BOM of the CCTV Camera (Analog)		
3.0	Optics	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Optics shall not exceed 10 % of the total BOM of the CCTV Camera (Analog)		
4.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property		

		Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table> <tr> <th>2023-24 & 2024-25</th><th>2025-26</th><th>2026-27 onwards</th></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
6.0	Housing (Plastic /Aluminium/MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed to 15 % of the total BOM of the CCTV Camera (Analog).						
7.0	Connecting Cables & Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BOM of the CCTV Camera (Analog).						
8.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10% of the total BOM of the CCTV Camera.						

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1) Main PCB and (Sr. No.8) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.3 Mechanism for calculation of local content of CCTV Camera (IP):

The domestic BOM of CCTV Camera (IP) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (IP)	Value addition / local content required for the input to be classified as domestic BOM
	1	2
1.0	Main PCB* with Capture and/or Processor Card	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BOM of the CCTV Camera (IP)
(i)	Network Interface Card (optional)	
(ii)	Infrared (IR) Board (optional)	
(iii)	I/O Board (optional)	
(iv)	Power over Ethernet (PoE) Card (optional)	
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BOM of the CCTV Camera (IP)
3.0	Optics	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Optics shall not exceed 10 % of the total BOM of the CCTV Camera (IP)
4.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation,

		prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table> <tr> <th>2023-24 & 2024-25</th><th>2025-26</th><th>2026-27 onwards</th></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
5.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table> <tr> <th>2023-24 & 2024-25</th><th>2025-26</th><th>2026-27 onwards</th></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
6.0	Housing (Plastic / Aluminium / MS) and	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 15 % of the total BOM of the CCTV Camera (IP).						
7.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BOM of the CCTV Camera (IP).						
8.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of Final Assembling and Testing shall not exceed 10% of the total BOM of the CCTV Camera (IP)						

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 8.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.4 Mechanism for calculation of local content of CCTV Camera (Analog Speed Dome):

The domestic BOM of CCTV Camera (Analog Speed Dome) would be the sum of the costs of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (Analog Speed Dome)	Value addition required for the input to be classified as domestic BOM
	1	2
1	Main Controller Board*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main Controller Board/Main PCB with/without optional boards shall not exceed 10 % of the total BoM of the CCTV Camera (ASD)
(i)	I/O Board (optional)	
(ii)	Infrared (IR) Board (optional)	
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total

		BoM of the CCTV Camera (ASD)						
3.0	Inhouse R&D#	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:						
		<table> <tr> <th>2023-24 & 2024-25</th><th>2025-26</th><th>2026-27 onwards</th></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
4.0	In-house Design/IPR#	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:						
		<table> <tr> <th>2023-24 & 2024-25</th><th>2025-26</th><th>2026-27 onwards</th></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
5.0	Housing (Plastic/ Aluminium/ MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the CCTV Camera (ASD).						
6.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BoM of the CCTV Camera (ASD).						
7.0	Motor, Heater & Blower, Zoom Module, Belt, Plastic Mechanism Parts, Glass etc.	Domestically manufactured from imported / domestically manufactured input parts and mechanical components. However, the weightage of the total value of all these parts/components shall not exceed 5% of the total BoM of the CCTV Camera (ASD)						
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Power Adapter" will be minimum 40% (of the total value of parts and components used in the manufacture of "Power Adapter"). However, the weightage of the total value of "Power Adapter" shall not exceed 5% of the total BoM of the CCTV Camera (ASD)						
9.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BoM of the CCTV Camera (ASD)						

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 3.0 (In-house R&D) & Sr. No. 4.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.5 Mechanism for calculation of local content of CCTV Camera (IP Speed Dome):

The domestic BOM of CCTV Camera (IP Speed Dome) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (IP Speed Dome)	Value addition / local content required for the input to be classified as domestic BOM		
	1	2		
1.0	Main Controller Board*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main Controller Board with/without optional boards Shall not exceed 10 % of the total BoM of the CCTV Camera (IPSD)		
(i)	I/O Board (optional)			
(ii)	Infrared (IR) Board (optional)			
(iii)	Processor Card (optional)			
(iv)	Network Interface Card (Optional)			
(v)	Power over Ethernet (PoE) Card (optional)			
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BoM of the CCTV Camera (IPSD)		
3.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources /expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
4.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	Housing (Plastic / Aluminium / MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the CCTV Camera (IPSD).		
6.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BoM of the CCTV Camera (IPSD).		
7.0	Motor, Heater & Blower, Zoom Module, Belt, Plastic Mechanism Parts, Glass etc.	Domestically manufactured from imported / domestically manufactured input parts and mechanical components. However, the weightage of the total value of all these parts/components shall not exceed 5% of the total BoM of the CCTV Camera (IPSD).		
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the		

		assembly of “Power Adapter” will be minimum 40% (of the total value of parts and components used in the manufacture of “Power Adapter”). However, the weightage of the total value of “Power Adapter” shall not exceed 5% of the total BoM of the CCTV Camera (IPSD)
9.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BoM of the CCTV Camera (IPSD)

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 3.0 (In-house R&D) & Sr. No. 4.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.6 Mechanism for calculation of local content of DVR/ NVR:

The domestic BOM of DVR/ NVR would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr No.	Main inputs in BOM / stages for manufacture of DVR / NVR	Value addition / local content required for the input to be classified as domestic BOM						
	1	2						
1.0	Main PCB*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BoM of the DVR/NVR.						
(i)	Front Panel & LED Board (optional)							
(ii)	I/O Board (optional)							
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BoM of the CCTV Camera (DVR/NVR)						
3.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.: <table> <tr> <td>2023-24 & 2024-25</td><td>2025-26</td><td>2026-27 onwards</td></tr> <tr> <td>7%</td><td>10%</td><td>12%</td></tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
4.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						

		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	Housing (Plastic / Aluminium / MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the DVR/NVR.		
6.0	Connecting Cables, Connectors and USB Mouse	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables, Connectors and USB Mouse shall not exceed 5% of the total BoM of the DVR/NVR.		
7.0	Remote Control	Domestic assembly* and testing from imported / domestically manufactured parts and components subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Remote Control" will be minimum 20% (of the total value of the parts and components used in the manufacture of "Remote Control") in Year 2, which will increase to minimum 30%, 40% and 50% in Financial Years 2025-26, 2026-27 and 2027-28 onwards respectively.		
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Power Adapter" will be minimum 40% (of the total value of parts and components used in the manufacture of "Power Adapter"). However, the weightage of the total value of "Power Adapter" shall not exceed 5% of the total BoM of the DVR/NVR.		
9.0	Final Assembly and Testing	Domestically assembled/tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BOM of the DVR/NVR.		

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

5. The surveillance devices i.e., CCTV Cameras (Analog/ IP/ Analog Speed Dome/ IP Speed Dome) should comply with the Essential Requirements (ERs) for security prescribed by MeitY to ensure the security of the VSS / CCTV systems, as per the Appendix 'A', as amended from time to time. The security testing report 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. These Essential Requirements (ERs) for security of CCTV Cameras/VSS system will be enforced after 3 months from the date of issuance of this Notification. The security norms for the DVR and NVR will be notified subsequently.

6. The notification will come into effect after 3 months from the date of issuance of this Notification. This Notification shall remain valid till the revised Notification is issued. The Year 1 for the purpose of this notification would be upto 31.03.2025.

7. No Electronic Product Notification under the Public Procurement (Preference to Make in India) Order 2017 shall have retrospective effect.

8. Purchase Preference shall be provided as per the provisions cited in the Public Procurement (Preference to Make in India) Order 2017 dated 16.09.2020 and, as amended from time to time, for the procurement of aforesaid electronics products.

9. The notification would also be applicable to all Central Schemes (CS)/ Central Sector Schemes (CSS) for the procurement of electronic products made by States and local bodies, if project or scheme is fully or partially funded by Government of India.

10. Procedure for calculating local content/ domestic value addition

10.1 Bill of Material sourced from domestic manufacturers (Dom-BOM) may be calculated based on one of the followings depending on data available:

- a) Sum of the costs of all inputs which go into the product (including duties and taxes levied on procurement of inputs except those for which credit/ set-off can be taken) and which have not been imported directly or through a domestic trader or an intermediary.
- b) Ex-Factory Price of product minus profit after tax minus sum of imported Bill of Material used (directly or indirectly) as inputs in producing the product (including duties and taxes levied on procurement of inputs except those for which credit/ set-off can be taken) minus warranty costs.
- c) Market price minus post-production freight, insurance and other handling costs minus profit after tax minus warranty costs minus sum of Imported Bill of Material used as inputs in producing the product (including duties and taxes levied on procurement of inputs except those for which credit / set-off can be taken) minus sales and marketing expenses.

10.2 Total Bill of Material (Total BOM) may be calculated based on one of the following depending on data available:

- a) Sum of the costs of all inputs which go into the product (including duties and taxes levied on procurement of inputs except those for which credit / set-off can be taken).
- b) Ex-Factory Price of product minus profit after tax, minus warranty costs.
- c) Market price minus post-production freight, insurance and other handling costs minus profit after tax, minus warranty costs minus sales and marketing expenses.

10.3 The percentage of domestic value-addition may be calculated based on information furnished as per the following formula:

Percentage of local content/ domestic value-addition = [(Dom-BOM) / (Total BOM)]*100

11. Verification of local content/ Domestic Value Addition

11.1. The local supplier at the time of tender, bidding or solicitation shall provide self-certification that the item offered meets the minimum local content and shall give details of the location(s) at which the local value addition is made.

11.2. In cases of procurement for a value in excess of Rs.10 crore, the local supplier shall provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

11.3. In case a complaint is received by the procuring agency or the concerned Ministry/Department against the claim of a bidder regarding local content/ domestic value addition in an Electronic Product(s), the same shall be referred to STQC.

11.4. Any complaint referred to STQC shall be disposed of within 4 weeks. The bidder shall be required to furnish the necessary documentation in support of the domestic value addition claimed in an Electronic Product(s) to STQC. If no information is furnished by the bidder, such laboratories may take further necessary action, to establish the bonafides of the claim. In case of the discrepancies in computation of local content, a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) for calculating the percentage of local content will supersede over the self-declaration certificate.

11.5. A complaint fee of Rs.2 Lakh or 1% of the value of the domestically manufactured Electronic Products being procured (subject to a maximum of Rs. 5 Lakh), whichever is higher, to be paid by Demand Draft to be deposited with STQC. In case, the complaint is found to be incorrect, the complaint fee shall be forfeited. In case, the complaint is upheld and found to be substantially correct, deposited fee of the complainant would be refunded without any interest.

11.6. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules (GFR) for which a bidder or its successors can be debarred as per Rule 151 (iii) of the General Financial Rules along with such other provisions of bidding, debarment by a single Ministry/Department and revocation of orders as per the Department of Expenditure O.M-No. F.1/20/2018-PPD dated 2nd Nov, 2021 may be permissible under law amended from time to time.

12. MeitY shall be the Nodal Ministry to monitor the implementation of the Electronic Products notifications. In case of any dispute/clarifications against the decision given by STQC, a committee is constituted with the following

compositions for verification/vetting the complaints, independent verification of self-declarations and auditor's/accountant's certificates on random basis, restrictive and discriminating terms and conditions against the domestic manufactures of Electronics Products(s): -

- | | | |
|------|--|--------------------|
| i) | Group Coordinator/Scientist- 'G' (IPHW) | - Chairperson |
| ii) | Scientist-'G'/Scientist-'F' from STQC | - Member |
| iii) | Scientist- 'E' or above from Cert-In/Cyber Division | - Member |
| vi) | Any other member(s) as co-opted by the Chairperson - | Member |
| v) | Representative from IPHW Division | - Member Secretary |

13. In case of a question whether an item being procured is an Electronic Product(s) to be covered under the Public Procurement (Preference to Make in India) Order 2017, the matter would be referred to the Ministry of Electronics and Information Technology for clarification.

[F. No. W-43/11/2021-IPHW]

ASHA NANGIA, Group Coordinator & Scientist 'G'

Appendix 'A'

Essential Requirement(s) for Security of CCTV

Securing a CCTV (Closed-Circuit Television) system is crucial to protect sensitive information and ensure the system operates effectively. Key areas of testing include exposed network services, device communication protocols, physical access to the device's UART, JTAG, SWD, etc., the ability to extract memory and firmware, firmware update process security and storage and encryption of data. Here are brief requirements for the security of a CCTV system:

- 1) Physical Security - Use tamper-resistant camera enclosures and locking mechanisms to deter physical tampering.
- 2) Access Control by Authentication, Role-Based Access Control (RBAC) and regularly review and update access permissions to reflect personnel changes.
- 3) Network Security by employing encryption of data transmission
- 4) Software Security by Regular Updates, Disable Unused Features and Strong Password Policies
- 5) Penetration Testing: Employ penetration testing to assess the system's resistance to cyberattacks and address vulnerabilities.

Essential Security Requirements

Sr. No.	Category	Testing Parameter	What to be tested	Documents Required
1)	Hardware Level Security Parameter (supported by software)	1.1 Verify that application layer debugging interfaces such as USB, UART, and other serial variants are disabled or protected by a complex password.	1. Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test 2. Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation 3. Testing, in presence of	1. Datasheet of the SoC being used in the device. 2. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. 3. Process flow of the Manufacturing/Provisioning of the device

		<p>OEM team, to verify the enabling/disabling of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware based debuggers and access control mechanisms in case the interface is enabled.</p> <p>4. Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning.</p> <p>[For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peripherals.]</p>	
	1.2 Verify that cryptographic keys and certificates are unique to each individual device.	<p>Identifying all the keys and certificates being used in the device eco-system and verification through:</p> <ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	<p>1. List of all keys and certificates being used in the device ecosystem</p> <p>2. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation)</p>
	1.3 Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and configured appropriately.	<p>1. Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test</p> <p>2. Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation</p> <p>3. Testing, in presence of OEM team, to verify the enabling/disabling of all the</p>	<p>1. Datasheet of the SoC being used in the device.</p> <p>2. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same.</p> <p>3. Process flow of the Manufacturing/Provisioning of the device</p>

		<p>ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware based debuggers and access control mechanisms in case the interface is enabled.</p> <p>4. Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning.</p> <p>[For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peripherals.]</p>	
	1.4 Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.	<p>Identifying whether TEE/SE/TPM is available or not in the device through the SoC datasheet and technical documentation submitted by the vendor.</p> <p>Further assessment is done on the basis of scenarios as applicable to device as defined below:</p> <p>CASE 1: TEE/SE/TPM is not available:</p> <p>No further assessment</p> <p>CASE 2: TEE/SE/TPM is available and enabled:</p> <p>Verification through code-review that crypto functions are called through TEE/SE/TPM APIs.</p> <p>CASE 3: TEE/SE/TPM is available but not enabled by the vendor:</p> <p>Termed as non-conformance to the requirement. OEM is required to enable and implement the TEE/SE/TPM.</p>	<p>1. Datasheet of the SoC being used in the device.</p> <p>2. User manual/ Technical specifications of the device</p> <p>3. Code snippets of the TEE API call, wherever applicable</p>
	1.5 Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM,	<p>Identifying all the keys and certificates being used in the device eco-system, sensitive data and their storage mechanism(s); and verification through:</p>	<p>1. List of all keys and certificates being used in the device ecosystem</p> <p>2. List of all the sensitive data with their intended usage and secure storage</p>

		TEE (Trusted Execution Environment), or protected using strong cryptography.	<ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	<p>mechanism(s) as implemented along with secure configurations to be enabled in the device.</p> <p>3. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation) private keys and certificates.</p>
		1.6 Verify the presence of tamper resistance and/or tamper detection features.	Testing, in presence of OEM team, to verify the measures implemented in the device to prevent software and hardware tampering.	<p>1. Measures available in the device to prevent software tampering.</p> <p>2. Measures available in the device to prevent hardware tampering.</p>
		1.7 Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.	Testing, in presence of OEM team, to verify the enabling of the Intellectual Property protection technologies provided by the chip manufacturer, if available.	<p>1. Datasheet of the SoC</p> <p>2. Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer which have been enabled.</p> <p>3. In case, no Intellectual Property protection technologies are being provided by the chip manufacturer, then a declaration stating the same.</p>
		1.8 Verify the device validates the boot image signature before loading.	<p>Testing, in presence of OEM team, to verify the following:</p> <p>1. Device boots up successfully with the documented secure boot process when a valid boot image is provided.</p> <p>2. Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided.</p>	<p>1. Datasheet of the SoC</p> <p>2. Technical specifications of the device regarding secure boot (should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.)</p>
		1.9 Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number	<p>Verification of the documentation provided by the vendor regarding the random number generators being used in the device.</p> <p>Verification through code-review that random number generators or related</p>	<p>Documentation regarding the random generators (either hardware based or software based or both) being used in the device with their intended usage.</p> <p>In case, hardware based random number generators are being used, vendors</p>

		generators).	libraries as applicable are being used in the device.	shall submit the following: 1. Datasheet of the SoC 2. Technical specifications of the device regarding random generators In case, software based random number generators are being used, vendors shall provide the libraries being used for the same.
2)	Software/Firmware	2.1 Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.	Testing, in presence of OEM team, to verify the declared memory protection controls available and enabled in the device using command line-based tools/commands or any other open-source tool like DEP, EMET tool.	Declaration of the memory protection controls available and enabled in the device.
		2.2 Verify that the firmware apps protect data-in-transit using transport layer security.	<p>1. Verifying that strong encryption algorithms and secure TLS version is supported by the device to establish secure communication.</p> <p>2. Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with.</p> <p>3. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites.</p> <p>4. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval.</p> <p>5. Verifying that the TLS session(s) are resistant to attempts of interception and decryption of network traffic using man-in-the-middle attacks using tools like Burpsuite.</p>	Specifications and documentation related to the configurations available in the applications and firmware related to transport layer security.
		2.3 Verify that the firmware apps validate the digital signature of server connections.	<p>1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following:</p> <ul style="list-style-type: none"> Security features, related to secure server connections and digital 	Document mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the

			<p>signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough.</p> <ul style="list-style-type: none">• Proper certificate validation, certificate chain validation and certificate revocation checks are implemented in the device. <p>2. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites.</p> <p>3. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval.</p> <p>4. Verifying that TLS session(s) are resistant to attempts of interception and decryption of network traffic using man-in-the-middle attacks using tools like Burpsuite.</p>	server connections.
	2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	<p>Secure code review [both automated and manual], in presence of OEM team, using a licensed static analysis tool through any of the following approaches:</p> <p>1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended]</p> <p>2. Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code review activity in the presence of representatives of evaluation agency.</p>	<p>1. Firmware binaries for code review.</p> <p>2. Internal code review reports</p>	

			<p>3. Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them.</p> <p>4. Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.</p>	
		2.5 Verify that each firmware maintains a software bill of materials cataloging third party components, versioning, and published vulnerabilities.	<p>Verification of the submitted list of third-party components by running automated tools like FACT on the firmware.</p> <p>Identifying vulnerabilities in the third-party component(s) through publically available vulnerability databases</p> <p>Verification and validation of the process defined by the vendor for providing regular security updates and patches for the firmware to address any known vulnerabilities in third-party components.</p>	<p>1. Documentation for information on software bill of materials, including third-party components and versions.</p> <p>2. Organization process and policies for the following:</p> <ul style="list-style-type: none"> Addressing and patching any identified vulnerabilities in third-party components. Informing the customers about the security issues or vulnerabilities and providing security updates and patches for the same. <p>3. Configuration management system and related policies for maintaining firmware and third-party binaries, libraries and frameworks along with the patches/fixes issued to the devices.</p>
		2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	<p>Independent secure code review [both automated and manual] using a licensed static analysis tool through any of the following approaches:</p> <p>1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems.</p>	<p>1. Firmware binaries for code review.</p> <p>2. Internal code review reports</p>

			<p>[Recommended]</p> <p>2. Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code review activity in the presence of representatives of evaluation agency.</p> <p>3. Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them.</p> <p>4. Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.</p>	
		2.7 Verify that the firmware apps pin the digital signature to a trusted server(s).	<p>1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following:</p> <ul style="list-style-type: none"> • Security features, related to secure server connections and digital signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough. • Proper certificate validation, certificate chain validation and certificate revocation checks are implemented in the device. 	Document mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.
		2.8 Verify security controls are in place to hinder firmware reverse engineering (e.g. removal of verbose debugging symbols).	Testing, in presence of OEM team, to verify the security controls as provided by the vendor to hinder firmware reverse engineering.	Documentation regarding the security controls in place to hinder firmware reverse engineering.
		2.9 Verify that	Testing, in presence of	Measures implemented in

		the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.	OEM team, to verify the measures implemented in the device to make it resistant to time-of-check vs.time-of-use attacks.	the device to make it resistant to time-of-check vs. time-of-use attacks.
		2.10 Verify the device uses code signing and validates firmware upgrade files before installing.	Testing, in presence of OEM team, to verify the following: i) Device gets successfully updated with the documented secure upgrade process when a valid update package is provided. ii) Device does not boot up when a tampered update package (like with missing signature, invalid signature) is provided.	Process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.
		2.11 Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Testing, in presence of OEM team, to verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.
		2.12 Verify that firmware can perform automatic firmware updates upon a predefined schedule.	Verification shall be done as per the applicable scenario: Case 1: Automatic OTA updates are available: A standard operating procedure for issuing automatic updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency as per C20, C21 and C22 security requirement. Case 2: Automatic OTA updates are not available and vendor provides manual updates: A standard operating procedure for issuing manual updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the	1. Modes of updates available i.e. automatic, manual or both. 2. Organizational process and policies regarding the issuing of updates to the devices.

			evaluation agency as per C20, C21 and C22 security requirement.	
3)	Secure Process Conformance	3.1 Verify that wireless communications are mutually authenticated.	Testing, in presence of OEM team, to verify the process of mutual authentication as laid down in the documentation by the vendor.	The documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.
		3.2 Verify that wireless communications are sent over an encrypted channel.	Identifying all the security mechanisms being used in the communication process verification through: <ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	Documentation regarding the security measures implemented in the device to prevent tampering of the data being sent through wireless mode of communication. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.
		3.3 Verify that whether trusted sources are being used for sourcing the components of the device i.e. trusted supply chain through a managed Bill of materials for critical hardware components (related to security functions like SoC) is in use.		Bill of materials for critical hardware components (related to security functions like SoC).
		3.4 Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption,		Supply chain risk identification, assessment, prioritization, and mitigation documents. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents.

		post-incident summary documents need to be submitted and demonstrate the same.		
		3.5 Verify the no proprietary network protocols are being used in the device. If yes, then complete implementation details and the source code for the same shall be provided.		Document for Network protocols used in the device.
4)	Security Conformance at product development stage	4.1 Design and architecture details till the PCBA and SoC level to be provided to aid in counterfeit mitigation and malware detection.		Design and architecture documents till the PCBA and SoC level.
		4.2 Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.	Process and method artifacts need to be submitted and demonstrate the same.	
		4.3 One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes. Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date	List of components that have been identified as requiring tracking targets of tainting/counterfeiting, CM tool. Quality assurance process need to be submitted and demonstrate the same.	

		malware detection tools).		
		4.4 Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.		Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.

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

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 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 Gazette 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.

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

Email**ASTETeleWorks RailwayBoard****Re: Fwd: Letter from Ministry of Railway for Ensuring security features in CCTV system at stations on Indian Railways -reg****From :** Arpita Datta <arpitad@stqc.gov.in>

Thu, Feb 15, 2024 05:25 PM

Subject : Re: Fwd: Letter from Ministry of Railway for Ensuring security features in CCTV system at stations on Indian Railways -reg 2 attachments**To :** ASTETeleWorks RailwayBoard <estet@rb.railnet.gov.in>**Cc :** Ranjit Kumar <edtd@rb.railnet.gov.in>, Suresh Chandra <suresh@stqc.gov.in>, Chittaranjan Das <cdas@stqc.gov.in>, Malabika Ghose <malabika@stqc.gov.in>, Sanjay KumarPrusty <sprusty@stqc.gov.in>

Sir,

This refers to your letter no. 2024/TeleDev/Security in CCTV System (3454081) dated 24-Jan-2024.

We shall conduct the proposed services in a phased manner.

Phase I:

a) Audit by STQC on Threat Modeling on the CCTV ecosystem and internal security Process Audit

Place: Railway Station of Howrah or Sealdah division

No. of days: 3

Service Charges: Rs. 90,000/- (local transport is to be arranged by you)

b) Vulnerability assessment of connected devices in the ecosystem

Already conducted for Bally (Eastern Railway), Byculia (Western Railway), Puducherry (Southern Railway)

Service Charges: Rs. 15,000/- per device (local transport is to be arranged by you)

c) Application security testing of applications deployed

As video surveillance applications are from different OEMs, we need that one of such applications is to be hosted at our laboratory before conduction of application security testing.

Service charges and number of audit days can only be estimated once we study the application.

Phase II:

Training to railway officials can be arranged at our laboratory.

No. of training days: 5

Training charges: Rs. 13,000/- per participant

Minimum no. of participants: 15

Probable training content:

a) Risk assessment of CCTV ecosystem

- b) Process audit based on ISO/IEC 27001: 2013 and 2022
- c) Vulnerability assessment based on CIS benchmark
- d) Application security testing covering security domains like authorization and access control, authentication, data and input validation, error handling, use of cryptography / data protection and secured configuration.

Pl. feel free to contact us if there is any query.

Regards,

Arpita Datta

Scientist 'F'

IT Services, Electronics Regional Test Laboratory (East)

STQC Directorate

Ministry of Electronics and Information Technology, Govt. of India

DN - 63, Sector- V, Salt Lake, Kolkata -700091

M: 9433060351

===== Forwarded message =====

From: Suresh Chandra <suresh@stqc.gov.in>

To: "Chittaranjan Dass" <cdas@stqc.gov.in>

Date: Wed, 14 Feb 2024 16:42:22 +0530

Subject: Fwd: Letter from Ministry of Railway for Ensuring security features in CCTV system at stations on Indian Railways -reg

===== Forwarded message =====

===== Forwarded message =====

From: M Vellaipandi <dgstqc@meity.gov.in>

To: "Suresh Chandra" <suresh@stqc.gov.in>

Date: Tue, 13 Feb 2024 13:02:35 +0530

Subject: Fwd: Letter from Ministry of Railway for Ensuring security features in CCTV system at stations on Indian Railways -reg

===== Forwarded message =====

Sir,

FYKI. Pl check and update on this.

Regards

एम वेल्लईपंडी/ M Vellaipandi

डी.जी. एस.टी.क्यू.सी. /DG STQC

सरकार भारत Govt. of India



भारत सरकार Government of India
रेल मंत्रालय Ministry of Railways
रेलवे बोर्ड (Railway Board)



No. 2020/TeleDev/ CCTV Projects (3322183)

Dated: 05.02.2024

General Manager
Zonal Railways,
Production Units

Director General
RDSO
Lucknow

Sub.: Regarding security verification testing of cameras and software at Stations.

Ref: (i) MeitY, Gol – OM no. W-43/6/2020-IPHW-MeitY, dtd. 25.08.2023 addressed to RDSO

(ii) MeitY, Gol – OM no 3(15)/2004-CERT-In (Vol. XIII) - Pt. dtd 21.11.2023 addressed to CRIS

(iii) MeitY, Gol – OM no W-43/6/2020-IPHW-MeitY dtd 08.01.2024 addressed to SWR

(iv) CSTE/Project/SWR's Letter no SG/SWR/Planning/2024/02 dtd 22.01.2024 to Railway Board

MeitY, vide its OMs referred above, has clarified the roles of CERT-In empanelled organization and specific expertise offered by STQC and also clarified that CERT-IN empanelled organizations are not assessed and empanelled by CERT-In for any product or hardware testing.

Since RDSO specifications need clarity on cyber security agency and the matter is concerned with security of entire Video Surveillance System (VSS) network of IR, in order to implement OMs of MeitY effectively, following directives is issued with the approval of Member (Infra), RB for immediate implementation:

“RDSO, RCIL & Zonal Railways are to procure CCTV Cameras as per RDSO specifications for critical locations/railway stations with security auditing & testing with STQC only in all ongoing & future projects wherever procurement is still to be materialize”.



(रणजीत कुमार)

कार्यकारीनिदेशक(दूरसंचारविकास)

रेलमंत्रालय

011-47843012, edtd@rb.railnet.gov.in

Copy to CMD/RCIL for information and necessary action pl.