Government of India
Ministry of Electronics & Information Technology
(Cyber Security and Cyber Law Group)

No. 20 (7)/2017-CLES Dated: 11/04/2018

Ref: Ministry of Electronics and Information Technology vide D.O. No 5(4)/2016-ESD dated 19/5/2017 issued Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations. The same is available at MeitY website (http://meity.gov.in).

Sub: CISOs Top Best Practices for a Safe & Secure Cyber Environment

1. Chief Information Security Officer's (CISO) Top Best Practices for a safe & secure Cyber environment are given below. It is strongly advised that all CISOs follow and implement the same.

    (i). **Know your IT environment** – Undertake an inventory of the computers and networked devices in your environment, types of data managed by your department, how these data-sets are classified, who has access, and their scale of importance and sensitivity? Maintain and update the threat landscape.

    (ii). **Build a Strong Internal Cyber-Hygiene Culture** – Educate, sensitize & train your employees on types of cybercrime attacks *and* safe cyber practices such as strong passwords, multi-factor authentication, secure Internet browsing, social media safety, use of USB sticks, etc.

    (iii). **Information Security Management System (ISMS)**: Identify, implement, operate, review and improve Information Security Policy for the department.

    (iv). **Implement Strong IT Asset Fundamentals** –

    a. Keep operating systems and software applications updated and patched from trusted sources on a regular basis. Ensure you have the latest OS / Versions / SW installed which have the latest security features inbuilt.

    b. Do not use software & hardware which are old, have no longer manufacturer's mainstream technical & product support or are near end-of-life support.

    c. Procure and use only genuine and current software & hardware from trusted sources to benefit from the latest security & privacy features.

(v). **Ensure a Robust Cybersecurity Policy Framework** – Implement and enforce a formal cybersecurity policy framework that includes governance, risk management, compliance, data back-up, enforcement and usage policy statements that clearly defines its purpose, guidance, roles & responsibilities.

(vi). **Deeper focus on User Identity & Information Security** – Protect and manage user identity and privileged access authentication with robust inbuilt identity & access management tools; Drive strong device protection with encryption & data leakage prevention; Maintain logs.

(vii). **Conduct Regular & Comprehensive Cybersecurity Reviews** – Undertake a regular and on-demand software asset management, cyber-risk analysis of your network, network resources and critical assets, threats and vulnerabilities, including audit of IT suppliers and vendors. Vulnerability Assessment & Penetration Testing (VAPT) of all websites and portals on quarterly basis at a minimum. Web Application Security Assessment (WASA) annually.

(viii). **Proactive Operations & Cyber Response Strategy** – Use tools and built-in technologies for active monitoring of network, devices and user activity to detect anomalies in systems processes, commands, registries, malware activity, unauthorized user behaviors, coupled with a cyber-response strategy involving – executive sponsorship, internal & external communication, threat containment & remediation, legal exposure & risk assessment.