

Cabinet Resolution No. (13) of 2023
Concerning the Committee for Preventing Cyber Threats and Malware

The Cabinet,

- Having reviewed the Constitution; and
- Federal Law No. (1) of 1972, Concerning the Competences of Ministries and the Capacities of Ministers, and its amendments thereof; and
- Federal Decree-Law No. (4) of 2004, Establishing and Regulating the Presidential Court, and its amendments thereof; and
- Pursuant to the proposal submitted by the Head of Cybersecurity for the UAE Government, and the Cabinet’s approval,

Resolved as follows:

Article (1)

Definitions

In application of the provisions of this Resolution, the following words and expressions shall have the meanings ascribed thereto, unless the context requires otherwise:

State	: United Arab Emirates.
Minister	: Deputy Prime Minister and Minister of the Presidential Court.
Committee	: Committee established under the provisions of this Resolution.
Concerned Authorities	: Federal or Local Authorities concerned with Electronic and Cybersecurity affairs in the State.
Cyber Threats	: Risks that person (natural/legal) face on the electronic network. The threat may be deliberate and planned, aiming at attempting to expose, change, disable, destroy, steal, or gain unauthorized access to assets, systems, infrastructure,

electronic networks, or information for personal, political, economic, subversive, or financial gain.

Malicious Software

: Malicious Software or applications that infect computers, electronic systems, or networks with the aim of violating their confidentiality, integrity, accuracy, and availability of data. These programmes block or obstruct access to the electronic system, encrypt files or data therein, or prevent the use of a computer or disable it or illegally access systems, software or the like.

Article (2)

Committee Establishment and Formation

1. A Committee called the "Cyber Threats and Malicious Software Committee" shall be established, affiliated to the Minister, and concerned with combating Cyber Threats and Malicious Software of all kinds.
2. The Committee shall be formed under the chairmanship of the Head of Cybersecurity of the UAE Government, with the membership of a representative of each of the following agencies:
 - a. Supreme Council for National Security (SCNS).
 - b. Ministry of Defence.
 - c. Ministry of Interior.
 - d. Ministry of Justice.
 - e. Federal Public Prosecution.
 - f. Signals Intelligence Agency (SIA).
 - g. Telecommunications and Digital Government Regulatory Authority (TDRA).
 - h. Abu Dhabi Digital Authority (ADDA).
 - i. Dubai Electronic Security Centre (DESC).
3. The Chairman of the Committee shall issue a decision naming the members of the Committee based on the nomination of the agencies referred to in this Article.
4. The Minister may add any other agencies to the membership of the Committee.

Article (3)

Committee's Competences

The Committee shall:

1. Study and propose legislation related to combating Cyber Threats and malicious software and proposing appropriate mechanisms to deal with risks and threats and related crimes.
2. Coordinate with the Competent Authorities and concerned parties to ensure protection and support for those affected by Cyber Threats and malicious software.
3. Prepare and study reports on the procedures used to combat Cyber Threats and malicious software, in coordination with the Concerned Agencies in the State, and submit them to the Competent Authorities to take the necessary action.
4. Establish a special and unified data record on Cyber Threats and Malicious Software and combating related crimes.
5. Receive complaints and notices from all federal and local authorities in the event that any of them were attacked by Cyber Threats and Malicious Software.
6. Follow-up with the Concerned Agencies and Authorities regarding combating Cyber Threats and Malicious Software, prevent or limit their effects, and find ways to deal with them, and share the results at the national and international levels with the Relevant Authorities, as decided by the Minister.
7. Contribute to spreading culture and awareness regarding Cyber Threats and Malicious Software.
8. Hold conferences, seminars and training on Cyber Threats and Malicious Software and issue bulletins and circulars in cooperation and coordination with the Relevant Authorities.
9. Any other tasks or powers assigned to the Committee by the Cabinet or the Minister.

Article (4)

Working System of the Committee and its Rapporteur

1. The Committee shall have a Rapporteur, who shall be selected, and his duties shall be determined by a decision of the Committee Chairman.
2. The Committee shall establish its working system, including a quorum for attendance and voting on its decisions.

Article (5)

Committee Powers

In order to exercise its competencies stipulated in this resolution, the Committee shall do the following:

1. Communicate and coordinate with the Competent Authorities and concerned parties related to its field of work.
2. Form specialised work teams and Sub-Committees from among its members to carry out the tasks assigned to them by the Committee.
3. Seek the assistance of whomever it deems appropriate among the specialists and experts in its field of work to provide assistance, advice and clarifications.
4. Invite whomever it deems to be specialists, technicians, and research and studies centres to attend meetings and express opinions on technical issues without having the right to vote on its decisions.

Article (6)

Exposure to Cyber Threats and Risks

Any federal or local government agency that is exposed to cyber risks, threats, and malicious software shall notify the Committee as soon as possible and cooperate with the Committee in implementing directives and instructions to deal with the situation. The Committee shall deal with the notice with the necessary speed, taking into account the nature of the agency that is exposed to these Malicious Software and the expected risks and damages.

Article (7)

Financial Appropriations

The financial appropriations necessary for the Committee to carry out its functions shall be allocated from the Presidential Court.

Article (8)

Resolution Publication and Entry into Force

This Resolution shall be published in the Official Gazette and shall come into force as of the date of its issuance.

Mohammed Bin Rashid Al Maktoum

Prime Minister

Issued by Us:

Issued on 10 Shaaban 1444 A.H.

Corresponding to: 02 March 2023 AD