RFC 2350 MIL.CERT-UA Description

Version 2.0 – August 2026

TLP:CLEAR

Table of Contents

1. Document Information

1.1 Date of last update

This is version 2.0, published on 03 August 2026.

1.2 Distribution List for Notifications

MIL.CERT-UA does not currently maintain a public distribution list for notifications of changes to this document.

1.3 Locations Where This Document May Be Found

The current version of this document is publicly available and can be found at:

https://mil-cert.gov.ua/en/about/rfc-2350

1.4 Authentication of This Document

This document is digitally signed using the MIL.CERT-UA OpenPGP key. The signature is available via the official website: mil-cert.gov.ua.

2. Contact Information

2.1 Name of the Team

MIL.CERT-UA – Cyber Defence Center – is the official Computer Emergency Response Team of the Ministry of Defence of Ukraine.

2.2 Address

MIL.CERT-UA

6 Povitrianykh Syl Avenue, Kyiv, 03168, Ukraine

2.3 Time Zone

UTC+2 (UTC+3 during daylight saving time)

2.4 Telephone Number

+38 096 773 73 70

2.5 Electronic Mail Address

cert@mil.ua

This address should be used for:

- incident reporting
- vulnerability disclosure
- cooperation and coordination requests

2.6 Public Keys and Encryption Information

MIL.CERT-UA supports secure communication using OpenPGP.

Key ID: 0x9669A693

Fingerprint: A98B 426E F0AE C53C F167 1128 148E 0E3A 9669 A693

Key length: 4096-bit RSA

Creation date: 25 March 2025

Associated identity: MILCERT-UA <cert@mil.ua>

A subkey is also maintained for operational use.

All sensitive communications should be encrypted using this key. All outgoing messages from MIL.CERT-UA are digitally signed.

2.7 Team Members

Management of MIL.CERT-UA is carried out by the Directorate, formed by authorized representatives of the respective units. Operational functions are performed by a permanent operational team that provides round-the-clock monitoring, analysis, and response to cyber incidents. The personnel composition of MIL.CERT-UA is determined by separate regulatory documents and is not subject to public disclosure.

2.8 Other Information

Preferred contact method: e-mail

Alternative channels: Signal, telephone

Hours of operation: 24 hours per day, 7 days per week, 365 days per year

Encryption: strongly recommended for all sensitive data

Information sharing: conducted using the Traffic Light Protocol (TLP)

3. Charter

3.1 Mission Statement

MIL.CERT-UA is responsible for ensuring an appropriate level of cyber defence of the Ministry of Defence of Ukraine.

Its mission includes detection, analysis, coordinated response, protection of critical infrastructure, and strengthening cyber defence capabilities.

3.2 Constituency

MIL.CERT-UA serves information systems of the Ministry of Defence, Armed Forces networks, State Special Transport Service systems, and other defence-related systems.

3.3 Sponsorship and Affiliation

MIL.CERT-UA operates under the Cyber Defence Center of the Ministry of Defence of Ukraine.

3.4 Authority

MIL.CERT-UA is authorized to handle cybersecurity incidents, coordinate responses, classify incidents, and engage external partners.

4. Policies

4.1 Types of Incidents and Level of Support

MIL.CERT-UA addresses unauthorized access, malware, DoS, cyber espionage, insider threats, and data breaches.

Support levels include advisory support, coordination support, and full operational leadership.

4.2 Cooperation and Information Sharing

MIL.CERT-UA cooperates with national cybersecurity authorities, defence entities, and international CERTs including NATO.

4.3 Confidentiality and Data Protection

Information is handled according to Ukrainian legislation and internal policies. Sensitive information must be encrypted and shared on a need-to-know basis.

4.4 Communication and Authentication

Communication channels include e-mail, telephone, Signal, and secure internal networks. All sensitive communications must be signed and encrypted.

4.5 Traffic Light Protocol (TLP)

MIL.CERT-UA applies TLP for information classification and sharing to ensure controlled dissemination and proper handling.

4.6 Operational Model

MIL.CERT-UA operates remotely with designated facilities available when required.

5. Services

5.1 Proactive Services

MIL.CERT-UA provides security contact databases, advisories, training, vulnerability coordination, and support for exercises.

5.2 Incident Response

MIL.CERT-UA performs incident triage, coordination, resolution, mitigation, recovery, and post-incident activities including analysis and reporting.

6. Incident Reporting

Incidents should be reported via cert@mil.ua or via system administrators and responsible organizational units. Reports should include description, affected systems, timestamps, and indicators.

7. Disclaimers

MIL.CERT-UA makes every effort to ensure information accuracy but assumes no responsibility for errors, damages, or operational limitations.