Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/cybersecurity-acronym-glossary/

EXECUTIVE GUIDE ON A REFERENCE FOR COUNSEL, EXECUTIVES AND COMPLIANCE TEAMS

Cybersecurity Acronyms, Expanded and Explained

Security reports, audit findings and regulatory correspondence assume the reader already knows what CISA, DFARS, EDR and SIEM stand for. This glossary expands each one and explains what the acronym means for your decision.

The acronyms below are the ones that appear most often in the incident reports, assessments and regulatory letters our clients bring to us. The list was adapted from the original evestigate.com library, with selected definitions clarified October 7, 2026 and the framing revised October 30, 2026. For the larger current reference, including digital evidence, identity and operational technology terms, see the Cybersecurity & Forensics Glossary.

Where a definition was clarified against a primary source, these are the sources: ISACA Certified Information Systems Auditor; U.S. government CISA agency information; HHS HIPAA covered entity guidance; IETF deprecation of SSL 3.0; and IETF deprecation of older TLS versions. Which laws and standards actually apply to an organization is a matter for the responsible organization and its counsel.

For any acronym in your letter or report beyond this list, send us the sentence it appears in and a senior examiner will explain what it means for your obligations.

The Acronyms, From APT to TCP/IP

Read an acronym as a label and the records as the finding. An EDR product named in a report tells you a tool was present, and the examiner then checks which devices it covered; a reference to HIPAA or PCI DSS names a framework, and counsel and the examiner work out which obligations attach to your data. When the abbreviation in front of you carries a legal, contractual or operational consequence, ask the examiner what the records actually show.

APT

Advanced Persistent Threat. A sophisticated cyber attack normally aimed at large companies and government agencies that hold high value data such as manufacturing plans, designs, intellectual property and defense projects. APTs are ongoing by design and give the attacker prolonged access to exfiltrate data or deliver malicious software at will while evading detection.

© 2026 Global Digital Forensics, Inc. All rights reserved.

CISA

The abbreviation has two common meanings. ISACA's Certified Information Systems Auditor is a professional credential. The U.S. Cybersecurity and Infrastructure Security Agency is a federal agency. Determine which is intended from the document and its context.

CISSP

Certified Information Systems Security Professional, a widely recognized independent information security certification granted by the International Information System Security Certification Consortium. It is awarded to individuals who have demonstrated proficiency in the security of the design, architecture, controls and management of highly secure digital environments. Joseph Caruso and Robert Knudsen of Global Digital Forensics both hold it.

CISO

Chief Information Security Officer, the senior executive ultimately responsible for the security of an organization's data and digital assets.

DFARS

The Defense Federal Acquisition Regulation Supplement adds Department of Defense acquisition requirements to the FAR. The requirements that apply to a supplier depend on the solicitation, the contract clauses and the work involved.

DLP

Data Loss Prevention describes policies and tools that detect or restrict specified uses or transfers of sensitive data. Its coverage follows the configured sources, rules and supported channels, so an examiner reading DLP records confirms which channels were monitored before weighing what the alerts show.

HIPAA

The Health Insurance Portability and Accountability Act is a U.S. law. Its implementing Privacy, Security and Breach Notification Rules apply according to defined roles for covered entities and business associates, and counsel confirms which role, and so which obligations, a business holding health related information carries.

© 2026 Global Digital Forensics, Inc. All rights reserved.

ICS (Security)

ICS stands for Industrial Control System. ICS security is the safeguarding of industrial control systems, the integrated hardware and software that monitors and controls machinery and associated devices in industrial environments.

IoT

Internet of Things refers to connected physical devices with sensing, processing or actuation capabilities. Connectivity may be direct or through a gateway, and a device that sits behind a gateway with only a local address is part of it as well.

EDR

Endpoint Detection and Response collects supported endpoint telemetry and supports detection, investigation and response. Coverage depends on the product, agent, platform and configuration, so the examiner confirms which endpoints carried the agent and looks to the logs of routers, printers and other network connected devices separately.

NIST

The National Institute of Standards and Technology publishes technical standards and guidance, including the Cybersecurity Framework. Organizations use the framework as a voluntary reference for organizing and measuring risk management, and an assessor records how closely a program follows it.

PCI-DSS

The Payment Card Industry Data Security Standard addresses environments that store, process or transmit payment card data and the systems that can affect their security. Applicable scope and validation are determined through the relevant payment relationships and current PCI SSC documents.

SCADA

Supervisory Control and Data Acquisition refers to a computer system used to monitor or control a plant or equipment in infrastructure industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. SCADA systems also allow data to be gathered and analyzed in real time.

© 2026 Global Digital Forensics, Inc. All rights reserved.

SIEM

Security Information and Event Management describes software used to monitor, log, alert on and analyze security events in support of threat detection and incident response.

SOX

The Sarbanes Oxley Act of 2002 includes financial reporting, governance and internal control requirements for public companies. Applicability and required certifications depend on the entity and the provision. Its certifications address financial reports and the internal controls behind them, and they are read within that scope.

SSL

Secure Sockets Layer is the predecessor of Transport Layer Security. SSL 3.0 is deprecated, as are TLS 1.0 and 1.1. Current secure communication depends on supported protocol versions, configuration and certificate validation, and TLS is now the name of the current standard.

TCP/IP

Transmission Control Protocol/Internet Protocol is the set of protocols governing communication between all devices connected to the Internet. It dictates how information is packaged, sent and received, and how it reaches its destination.

When the Acronym Carries a Consequence

An acronym in an assessment or in a regulator's letter usually marks the point where a technical fact becomes a legal or contractual question: whether a DFARS clause reaches a subcontractor, whether a SIEM actually logged the account that was compromised, or whether a SCADA network was segmented the way the diagram claimed. Our critical infrastructure and OT security practice and our DFARS compliance work exist to examine those questions against the evidence. Global Digital Forensics has served counsel and businesses since 1992, our examiners hold credentials that include the CISSP, EnCE, CCE and CHFI, and the initial consultation is free. Call (800) 868-8189.

Web Addresses for the Sources Cited

1. ISACA Certified Information Systems Auditor: https://www.isaca.org/credentialing/cisa
2. U.S. government CISA agency information: https://www.usa.gov/agencies/cybersecurity-and-infrastructure-security-agency
3. HHS HIPAA covered entity guidance: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
4. IETF deprecation of SSL 3.0: https://www.rfc-editor.org/rfc/rfc7568.html

© 2026 Global Digital Forensics, Inc. All rights reserved.

5. IETF deprecation of older TLS versions: https://www.rfc-editor.org/rfc/rfc8996.html

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.