NDAA, GDPR Compliance & Next Level Cybersecurity

National Defense Authorization Act
WISENET
NDAA Compliant Products & Solutions

By Soumik Ghosh, Head of Product & Marketing, Hanwha Techwin India

Concerns about the ability of hackers to access live images or retrieve recorded images captured by video surveillance cameras located in security sensitive areas have been around for a while. Many manufacturers of professional level cameras have responded to the threat by introducing several methods to prevent. However, hackers are likely to continue to look at other ways to gain access to data, including via a camera's 'back door'.

There has been many topics or acronyms that are regularly used on websites and in documentation to describe the attributes of video surveillance products but none is more important than NDAA, GDPR and Cybersecurity.

On August 13, 2018, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA or the Act) (H.R. 5515) was signed into law.

Under the NDAA 2019 Section 889, federal agencies are prohibited from procuring video surveillance equipment and services from certain companies after August 13, 2019. The law also covers security equipment containing major components constructed by those banned companies like SoC (System on Chip) that are essentially the brain of your security camera or recorder.

Fortunately, with there being no shortage of non-blacklisted manufacturers offering professional-level video surveillance solutions, stakeholders can take advantage of a highly competitive marketplace to procure cameras & recorders that are cost-effective, as well as NDAA compliant.

Hanwha Techwin – Korean at heart

With its headquarters and manufacturing facilities in South Korea as well as in Vietnam, Hanwha Techwin has introduced a long list of products that are NDAA compliant and has been able to prove that none of its products includes components manufactured by any of the blacklisted companies.

GDPR

The Information Technology Act, 2000 (amended in 2008) provides for data protection through its various sections that enables the framework to govern data privacy in India.

With Wisenet cameras equipped with the Wisenet7 SoC meeting Secure by Default, as well as UL CAP standards, end-users can be assured that in addition to NDAA compliance, the cameras will also help them comply with GDPR by ensuring confidential data cannot be accessed, copied or tampered with.

Security as a Priority

The recent data breaches of Air India Domino's Pizza etc. are alarming.

Cybersecurity attacks impacted 52% of organizations in India over the last 12 months, according to a report by cybersecurity solutions provider Sophos and IT analysis, research and consulting firm Tech Research Asia (TRA). As many as 71% of these firms termed it "serious or very serious attack" and 65% said it took more than a week to fix, the report said.

The main legislation in India governing the cyber space is the Information Technology Act, 2000 ("IT Act") that have framed several rules under the Act such as CERT Rules, SPDI Rules & PDP Bills

At Hanwha Techwin, Cybersecurity is at the core of our solution always & is our number one priority, which is why our Security Vulnerability Response Center (S-CERT) is entirely focused on addressing any potential security vulnerabilities in our Wisenet products and solutions. A team in our Korean R&D center is dedicated to cybersecurity threat with effective countermeasures.

Our ground-breaking Wisenet7 SoC, includes a host of features such as Secure Boot Verification, Secure OS and Anti-Hardware Clone.

All our Wisenet7 products provide enhanced security out of the box at factory default settings. By default, the HTTPS mode is enabled, and unnecessary initial services are disabled, including SNMP (Simple Network Management Protocol), Link-Local address, UPnP discovery, and Bonjour. In addition, the SUNAPI & ONVIF protocols are disabled by default until a user password is configured. All Hanwha Techwin products ship without a default password. Wisenet7 products support the latest TLS version 1.3 for faster performance & enhanced security. Thus, we fully support the requirements of the 'Secure by Default' standard as an additional seal of trust to our products.

Soumik Ghosh
Head of Product & Marketing,
Hanwha Techwin India

> "In today's connected world, the importance of Act/Policy awareness like NDAA & GDPR and its effectiveness in preventing Video Surveillance equipment's being exposed to malicious cyberattacks."