VISIBILITY & COMPLIANCE WITH THE FAR SECTION 889 BAN

ARMIS

On August 13, 2020, the U.S. DoD, GSA, and NASA issued an interim rule amending the Federal Acquisition Regulation (FAR) to implement section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019. The interim rule addresses the new prohibition on "use" of banned telecommunications equipment and services and clarifies the prohibition on buying such equipment that went into effect in 2019. The interim rule prohibits federal agencies from doing business with any entity that uses telecommunications and video surveillance services or equipment from the following five vendors:

- Huawei Technologies Company
- ZTE Corporation (or any subsidiary or affiliate of such entities)
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company (or any subsidiary or affiliate of those entities)

There are a few critical aspects to be aware of with this manufacturer prohibition.

It prevents any company who is using equipment or services from these 5 companies or their affiliates from doing business with the Federal Government. It implements 2 compliance checks:

- Make a "reasonable inquiry" before submitting offers for work regarding its use of prohibited equipment or services.
- Identify and report on previously undisclosed use of prohibited equipment or services within 1-day and must also report mitigation taken within 10-days.

Even companies that provide healthcare, hospitality, insurance, and payroll services to the federal government are also subject to the new rule.

- Discovers all assets, including prohibited 889 manufacturers
- Identifies gaps, vulnerabilities & risks, including prohibited 889 devices
- Automates & enforces security policies
- No agent to install and 100% passive

5
Banned companies

291
Banned subsidiaries & affiliates

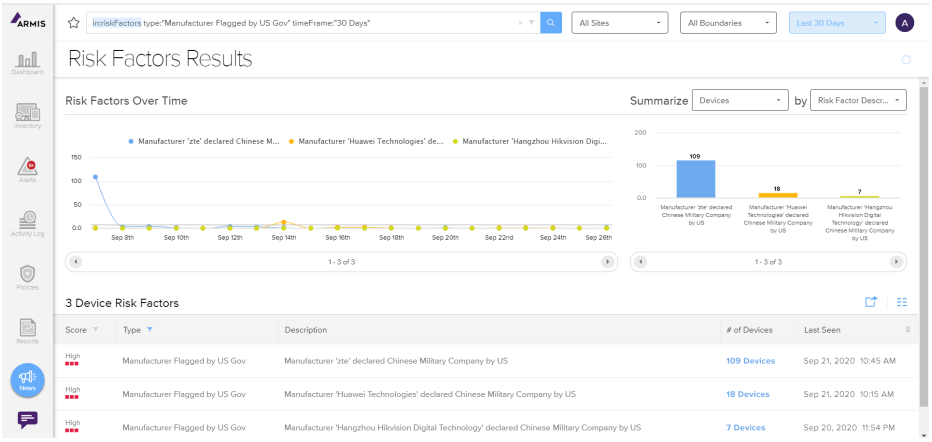
We actively discover and continuously monitor for devices, not just from the 5 core banned companies, but their 291 affiliates and subsidiaries.

 © 2020 ARMIS, INC.

Report In Minutes - Alert In Real Time

Armis can identify manufacturers whose devices are prohibited via our ability to identify and classify the devices, as well as compare with insights from our Device Knowledgebase. As an agentless and passive solution, there is nothing to install on devices, and no scanning of devices required. Armis can help ensure organizations doing work with the government are in compliance with the FAR Section 889 ban.

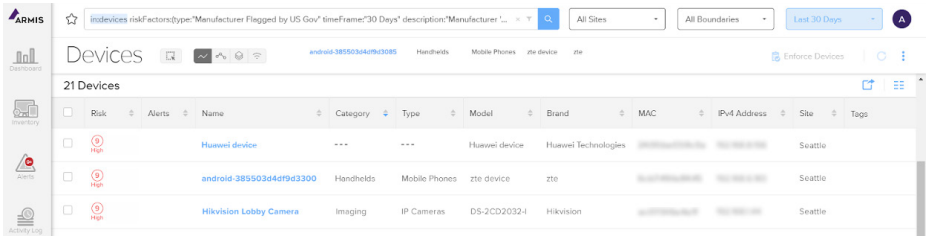
We actively discover and continuously monitor for any specific devices that are made by the 5 banned companies or their 291 subsidiaries & affiliates. We have risk factors that can identify the specific manufacturers flagged by the U.S.



Example of Armis Standard Query for "Manufacturer Flagged by U.S. Government" across an organization.

Government to let you know if you have any of the prohibited devices.

You can drill into reports to identify manufacturers in your environment for any such ban or prohibition. This gives you the ability to identify and take action for compliance in minutes.



Example of devices from the query.

VISIBILITY IN ACTION

The release of the Federal Acquisition Regulation Ban 889 has impacted many organizations, gaining visibility at the Board level. A CISO at one such Armis customer was in a Board meeting when the 889 Ban came up. There was significant concern not only about how they would be able to identify the impacted devices, and how critical it was to be able to show compliance, so that it did not negatively impact the business.

As the CISO had already implemented Armis, he ran a simple report and generated a list of devices from the flagged key companies in minutes, ensuring the Board that they could identify the devices, take action, and address Section 889.

"When Section 889 came up and we had to identify all of our Hikvision, Huawei and other Chinese manufacturers from our supply chain, there was a concern about how we would be able to identify them. Armis identified these devices in minutes, and we had the results to the Board the same day."

CISO, Fortune 100 Company

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

ARMIS

1.888.452.4011
armis.com

© 2020 ARMIS, INC.

20200929-2