SOLUTION BRIEF

NDAA Section 889 Compliance

Tanium can help your organization comply with the new U.S. National Defense Authorization Act (NDAA). Know what is on your network and protect your business.

Keeping the Nation Safe

The United States faces serious threats from foreign intelligence actors attempting to infiltrate domestic IT systems. To help keep the nation safe, the U.S. National Defense Authorization Act (NDAA) now includes two prohibitions against nefarious networks.

One of these NDAA rules — Section 889, Part A — prohibits the U.S. government from obtaining telecommunications equipment and services produced by selected Chinese companies. Part B of the same section applies to government contractors and suppliers. It prohibits them from contracting with any entity that uses these same Chinese telecommunications products and services.

As of today, few government agencies or contractors can comply. They lack the kind of visibility into systems that they need to identify noncompliant components. Yet time is running short. The first NDAA deadline arrives in August 2021.

The Trouble With Traditional Asset Discovery Tools for NDAA Compliance

Traditional asset discovery tools simply aren't up to the task of NDAA compliance. These legacy tools fall short because they:

- Can't (without extensive customization) provide a sufficiently granular view of IT assets down to the IP address, location and device type.
- Can't provide comprehensive visibility into the IT environment and are unable to discover certain subnetworks.
- Can't discover certain device types, such as security cameras, or cannot see all the way to the chip level that may be necessary for NDAA compliance.

Key Benefits

Maintain NDAA Compliance and Maintain Compliance and Security of Your Endpoint Devices

Accurately identify your noncompliant endpoint devices, allowing you to disable or replace them for NDAA compliance.

Help maintain compliance with NDAA, protecting your government contracts as well as your ability to bid on future government contracts, while also helping protect you against possible fines for noncompliance.

Improve collaboration between your IT operations and security teams. Tanium modules are designed to work well with both disciplines.

NDAA Compliance With Tanium

Tanium's modules can facilitate NDAA compliance by identifying devices on your network that are able to broadcast data.

- Tanium Platform modules, including Tanium Asset and Tanium Discover, provide endpoint management and endpoint security.
- Tanium modules can find and identify endpoint devices, but also detect and report on detailed hardware and software information utilized on the endpoint device.
- Tanium's tools are highly scalable. Tanium recently helped one customer uncover some 27,000 missing endpoints, all of which were previously unmanaged.
- Tanium's offerings are also available as a cloud-based service for out-of-the-box ease and speed.
- Tanium is partnering with multiple leading technology providers, system integrators and consulting firms to help support your NDAA compliance efforts.

How Tanium Helps Your Organization Comply With NDAA

The Tanium Platform in combination with the Tanium Discover module form the heart of Tanium's NDAA compliance offering.

The Tanium Platform unifies security and IT operations teams with a single view of critical endpoint data in real time. Because it's comprehensive and up-to-date, your organization can make informed decisions about NDAA compliance, then act with lightning speed to minimize disruptions to your business.

Tanium knows that NDAA compliance begins with knowing what's connected to your network. That's why Tanium's customers use Tanium Discover to scan their network for unmanaged assets. Administrators can then choose to block the devices or bring them under management.

For extra reporting and more granular information, you can also add Tanium Asset. It will give your IT operations and asset-management teams real-time data about your devices and their software, regardless of location. These rich insights can help your organization make the right decisions about managing your devices and systems for NDAA compliance.

Tanium can be integrated with other popular software-management tools. Tanium makes managing these other tools easier and more efficient, while unlocking greater insights.

Deliver Results From Day One

Tanium's offerings for NDAA compliance are available as a cloud-based service. With Tanium as a Service, all you have to do is deploy Tanium's software agents in your environment, then point them at the TaaS server. It's that simple — and that quick.

Speed matters, because the first deadline for reporting on NDAA is coming on Aug. 13, 2021. By that date, you'll need to tell the government whether you located any devices that potentially violate the new rules.

If you're already a Tanium customer, then it's simply a matter of making sure you have all the required modules. If you do, then you're ready to roll. If you need to add one more module, Tanium can help you do that quickly and efficiently.

The first deadline for reporting on NDAA is August 13, 2021.

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.