SEPIO

NDAA Section 889 Challenges

A Sepio Systems white paper

Overview of Section 889

Section 889 is part of the National Defense Authorization Act (NDAA) for Fiscal Year 2019. The statute imposes new restrictions on the procurement of telecommunications equipment or services from certain companies, and their subsidiaries or affiliates, based on their ties to the Chinese government. In doing so, the regulation expanded the list of forbidden products for federal contractors.

The aim of Section 889 is to protect National Security from cyber-attacks carried out by foreign adversaries. The US government has, on numerous occasions, accused the Chinese government of using its telecommunications operators for pernicious purposes – specifically, malicious activity aimed towards the US. According to Robert Bigman, former CISO at the CIA, "this [Section 889] was specifically as a result of intelligence that the US government had".

> ***"Section 889 was specifically as a result of intelligence that the US government had"***
>
> *Robert Bigman, former CISO @ CIA*

Section 889 prohibits the federal government, government contractors, and grant and loan recipients from procuring or using certain "covered telecommunications equipment or services" that are produced by Huawei, ZTE, Hytera, Hikvision and Dahua and their subsidiaries as a "substantial or essential component of any system, or as critical technology as part of any system". The statue does not have an exemption for commercial item contracting, thus the prohibition applies to all purchases regardless of the size of the contract or order. Section 889 is comprised of two parts:

Sec. 889(a)(1)(A)
(known as Part A)

Requires the federal government, as of August 13, 2019, to not "procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."

Sec. 889(a)(1)(B)
(known as Part B)

Since August 13, 2020, the federal government is prohibited from entering into or extending or renewing contracts with any entity that "uses any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."

Part B has a much broader impact on the government and its contractors due to the extensive and ambiguous language used in the statute. To put simply, Robert Bigman states that "people who are providing support to the contractors who are providing support to the government…they all have to comply". As such, under Section 889, contractors are required to present to the government, annually, whether the supplies or services that they offer include covered telecommunications equipment or services.

Supplies and services also include products that they use, but do not own, and is not limited to geographical boundaries, meaning that the geographical location of the equipment system or service, and the geographical location of its use, is irrelevant – all covered telecommunications equipment and services fall under the regulation.

Furthermore, contractors must report to the government when covered telecommunications equipment or services are in operation during contract performance. Section 889 proves to be a comprehensive regulation that aims to maintain US National Security as the attack surface increasingly moves towards the perilous cyber realm.

Compliance

In order to ensure compliance, the figure below provides a set of steps that, when followed, will assist contractors in their efforts to follow the new regulation.

01 **REGULATORY FAMILIARIZATION**

02 **"REASONABLE INQUIRY"**

03 **EDUCATION**

04 **REMOVAL**

05 **REPRESENTATION**

06 **CONTINUOUS REPORTING**

1. Regulatory familiarization

Contractors must first read, and attempt to understand, the rule and necessary actions for compliance. This is a fundamental step as it will make the rest of the process much smoother and reduce the likelihood of non-compliance that could arise as a result of misunderstanding the regulation itself.

2. "Reasonable Inquiry"

This is an inquiry that is designed to uncover any information about the identity of the producer or provider of covered telecommunications equipment or services used by the entity, or within its supply chain. Government stakeholders and contractors need to inventory their telecommunications equipment and evaluate their entire supply chain and acquisition procedures to identify prohibited equipment in their infrastructure. "Reasonable Inquiry" is the most crucial step, yet is a difficult task for legacy IT asset management (ITAM) tools due to their inability to discover, and fully identify, the manufacturers of every device across all environments – IT, OT, and IoT. Moreover, some organizations use multiple tools and patch together inventory reports which result in gaps in visibility. Government stakeholders need ultimate visibility into all hardware assets in order to detect the presence of prohibited covered telecommunications equipment or services.

3. Education

Organizations need to educate their purchasing/procurement and materials management professionals to ensure that they are familiar with the compliance plan. Moreover, the relevant IT/security teams need to receive continuous training regarding supply chain attack risks to raise their awareness of the entire attack surface.

4. Removal

Should covered telecommunications equipment or services be present within the organization, such equipment or services must be removed and replaced with 889-compliant devices.

5. Representation

Part A representations.

Offeror must make a representation stating whether it "will" or "will not" "provide covered telecommunications equipment or services to the government".

Part B representations.

Offeror must make a representation stating whether it "does" or "does not" "use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services".

If the offeror "will provide", or "does use", covered telecommunications equipment or services, the offeror must identify all such equipment or services and describe its proposed use under the contract. If the contractor "does use" covered telecommunications equipment or services, the prohibition applies regardless of whether or not that usage is performed under the federal contract, and where in the world it is being used.

6. Continuous reporting

Contractors must ensure there is continuous reporting to identify any instances where covered telecommunications equipment or services are present. If covered telecommunications equipment or services are discovered during the course of the contract performance, the contractor must report certain information to the contracting officer within one business day from the date of identification.

Failure to follow Section 889 will result in the organization failing to receive an 889-compliance certification. Consequently, the contractor will be unable to renew or extent existing contracts.

Possible Breaches

Erroneous incidents

An erroneous incident occurs when someone mistakenly connects a non-889 approved device to the organization's infrastructure. This can be common since it is difficult to determine the nature of a device simply by looking at it. Hence, education is imperative to avoid such incidents. With the relevant training and education, staff will be more aware of the various devices that should not be used within the working environment, including the at-home working environment. Staff training, however, cannot be relied upon as a sufficient cybersecurity measure on its own. Education might improve employees' awareness of cyber risks, but this cannot be a full-proof method to prevent attacks. Organizations must also rely on security software that assists in these efforts. When it comes to Section 889, organizations will benefit greatly from deploying software that provides complete device visibility as a non-889 approved device will be automatically detected, thus mitigating the risk of erroneous incidents.

Malicious actors

Often, cyberattacks are conducted by malicious actors who seek to cause damage to their target. As such, these cyber criminals employ highly sophisticated techniques that conceal their attack(s) by exploiting organizations' "blind spot" – device visibility. Bad actors may turn to man-in-the-middle (MiTM) methods and change a device's MAC address, packaging, or embed modules from a non-approved company and rebrand it as an 889-compliant product. By disguising itself, the organization is oblivious to the Rogue Device's presence within the infrastructure, unwittingly allowing it to remain there and potentially cause severe damage. It is therefore imperative that organizations have complete device visibility to know which devices are present within their infrastructure and, more importantly, the true identity of all devices.

Supply chain infiltration

Some targets, specifically government entities and their contractors, are very well protected and are therefore challenging to infiltrate directly. Hence, malicious actors commonly turn to the supply chain as their point of entry due to the less stringent security measures in place at some third parties. With supply chains often spanning hundreds of organizations, cyber criminals have various infiltration points that provide them with access to the target organization.

Inaccurate representation

If the contracting officer has reason to question the contractor's representation, further action can be taken to investigate the contractor's use of covered telecommunications equipment and services. If such an investigation finds that the contractor provided an inaccurate representation, this constitutes a breach of the Section 889 regulation. A case of inaccurate representation can also arise when an entity within the supply chain fails to disclose the use of covered telecommunications equipment and services. To avoid this, contractors must ensure that they undertake a diligent review of their internal processes and supply chains and identify any use of covered telecommunications equipment or services – the entire supply chain must disclose the use of any covered telecommunications equipment or services for there to be an accurate representation.

Risks of Non-compliance

Primarily, failure to comply with Section 889 will result in the termination or cancellation of the organization's contract with the federal government. However, a further consequence of non-compliance is a potential allegation of a False Claims Act violation. A violation of the False Claims Act is when a person or organization makes a false claim to the government and, concerning Section 889, this stems from inaccurate representation. Hence, the representation step of the compliance process is fundamental. A False Claims Act violation allegation can also be made when a supplier uses the prohibited technology and causes the organization to submit an inaccurate representation. Therefore, before making a representation to the contracting officer, the entire supply chain must be comprehensively evaluated. The consequence of a fine can be costly; up to $23,000 thus demonstrating the expense that comes with noncompliance.

Sepio Systems' HAC-1 Solution

With Section 889 in place, contractors need now, more than ever, complete device visibility. For comprehensive coverage, this is a challenging task that requires manual efforts to ensure that every device is accounted for. Even then, some devices may go undiscovered and, more worrisome, is that malicious devices will likely go undetected due to their extremely covert nature. The clandestine characteristics of Rogue Devices even illude security software solutions and thus continue to operate within the organization's infrastructure without being noticed.

Rogue Devices operating on the USB interface can disguise themselves as legitimate HIDs and therefore do not raise security alarms. Those which function on the network interface sit on the Physical Layer, which is not covered by existing security software solutions, and subsequently go undetected. With gaps in device visibility, contractors will be unable to detect and identify the true nature of all devices operating within their infrastructure. This vulnerability is a great cause for concern at any time, but especially in the case of Section 889 since this regulation was the result of intelligence that alluded to the fact that specific telecommunications equipment and services were being used for sabotage purposes. There needs to be complete device visibility for organizations to comply with Section 889 and obtain contracts and loans from federal agencies.

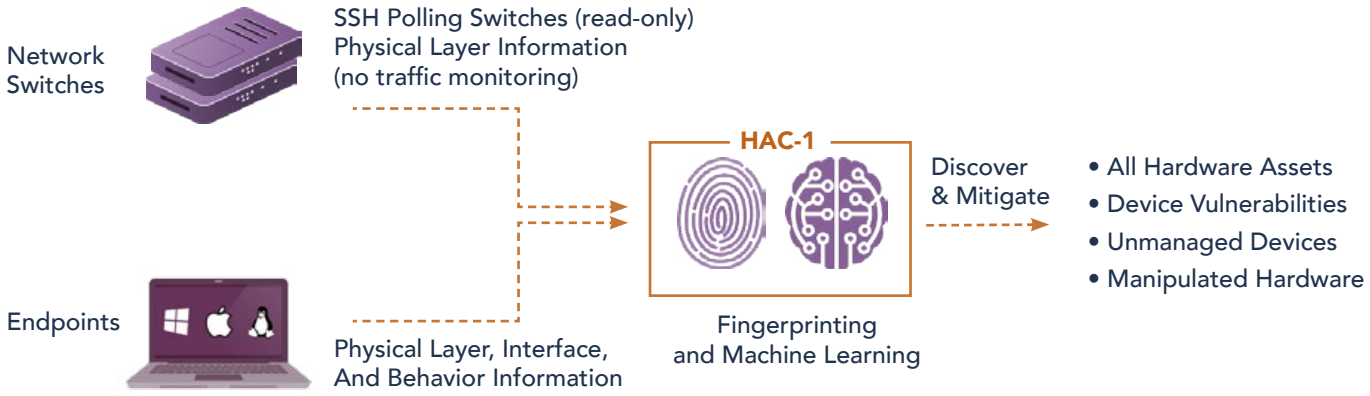
Sepio Systems has developed the HAC-1 solution which provides a panacea to the gap in device visibility. As the leader in Rogue Device mitigation, Sepio's solution discovers all devices operating over network and USB interfaces. The security software solution uses Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of the device and compares them against known fingerprints, automatically providing information on the vendor name, product name and more; including any abnormalities that could indicate the presence of a Rogue Device.

This is especially useful regarding Section 889, whereby the use of products manufactured by specific companies is prohibited. Moreover, with HAC-1 providing complete device visibility, organizations can prevent potential supply chain intrusions. In addition to detecting the presence of Rogue Devices, HAC-1 provides organizations with an automated mitigation process, based on a pre-set policy created by the system administrator, which blocks unapproved and Rogue hardware. As a result of deploying the HAC-1 solution, government stakeholders and contractors can, in real-time, monitor and maintain a state of compliance with the complicated Section 889 regulation.

The HAC-1 solution is comprised of three products:

HAC-1 Host	Provides Endpoint Security by guarding against Rogue Devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices. A Spoofed Peripheral impersonating a legitimate HID would be detected and blocked.
HAC-1 Port	Provides Network Security by polling switches to analyse the activities occurring on the Physical Layer. HAC-1 Port detects all Rogue Devices plugged into the Ethernet network, as well as any switch vulnerabilities and unmanaged network devices.
Sepio Agent	Orchestrates both Endpoint and Network Security by using hardware fingerprinting and Machine Learning, providing an alert for any security threats, as well as distributing the device usage policies.

How It Works



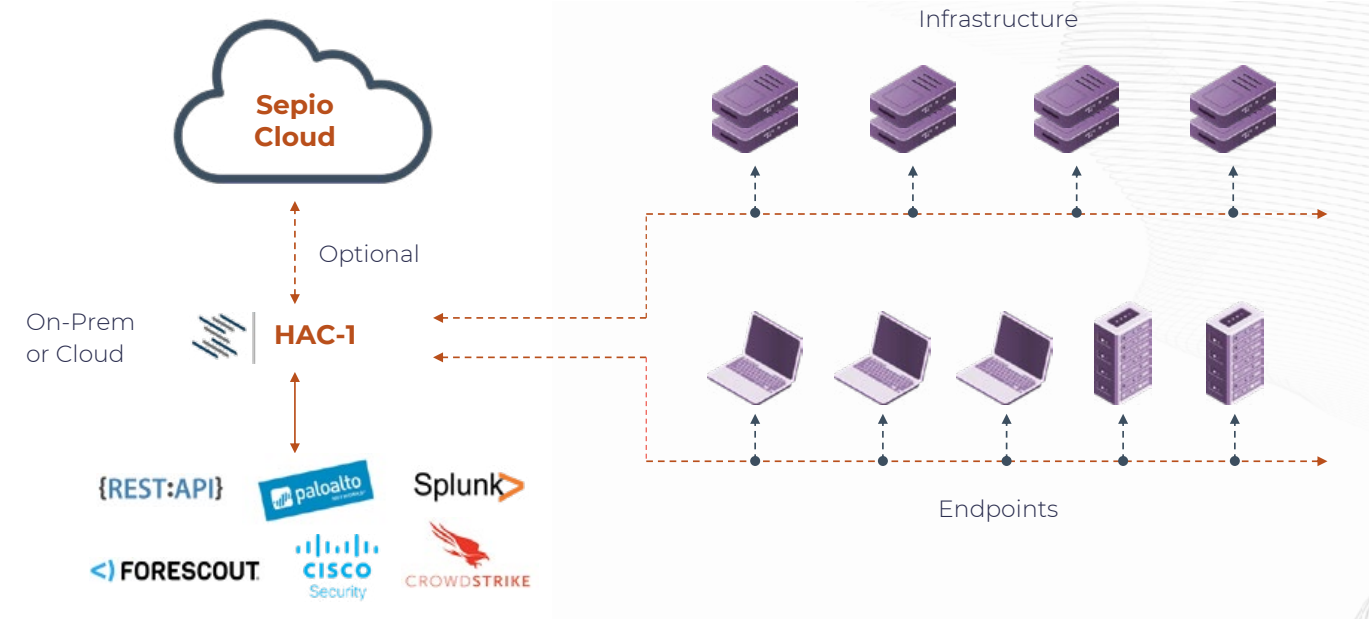
Deployment and Architecture

The Sepio Security Suite can be deployed 100% on-premises without any external components, or over a public or private cloud infrastructure. HAC-1 Port, which includes the Physical Layer implant detection module, requires SSH access to the organisation's network switches. The required privilege level for the assigned user is low as the solution requires only Read-Only "show" commands. Upon an implant/spoofed device being identified, a warning will be displayed, and an alert will be triggered – the mitigation is done by the solution's northbound interface either through its built in Syslog Legacy/CEF interface or, for those customers who operate a NAC solution, through their REST API option. The detection module does not probe user traffic and does not require a baseline to operate, so implants/spoofed devices may be detected even if they were present before the HAC-1 solution is deployed.

HAC-1 Host requires a lightweight agent installation on the endpoint; this agent does not conflict with other EPS solutions that may have been installed on the device. Once a policy and baseline has been set, ARM mode will be activated where ultimate USB protection will be enforced.

Sepio Agent, which facilitates the entire HAC-1 solution, is used in a Docker container environment and provides a web user interface for provisioning and policy configuration. The system administrator can lock a list of approved devices based on the existing and recognized devices, or on a known list of devices that were witnessed unharmful in other installations. Sepio Agent is completely autonomous and self-contained and is able to block entire peripherals or only functional parts (internal interfaces) instantly if they breach the pre-set policy.

System Architecture



Call for Action

In order to maintain and acquire government contracts, and loans and grants, organizations must ensure that they disclose whether or not they use covered telecommunications equipment or services. To do so, there needs to be ultimate device visibility. And with malicious cyber criminals discovering new ways to conceal their hardware attack tools, it is even more of a challenge for organizations to gain complete awareness of the true nature of all devices operating within its infrastructure.

Visit us at **www.sepio.systems** to find out more about our HAC-1 solution. Here, you can contact our sales team to further discuss the usage and benefits of HAC-1 in relation to Section 889 compliance. Additionally, we provide demos to give a visual representation of how our solution works once deployed. Please do not hesitate to reach out to us with any questions or inquiries.

We are also available on:

Linkedin >>

https://www.linkedin.com/company/sepio-systems/

Facebook >>

https://www.facebook.com/cybersepiosystems/

Twitter >>

https://twitter.com/sepiosys

LEARN MORE

SEPIO