IRS 1075 COMPLIANCE: WHY TRADITIONAL TOOLS FAIL TO SECURE UNMANAGED DEVICES

SOLUTION BRIEF

IoTSecure®

IRS 1075 Compliance: Why Traditional Tools Fail to Secure Unmanaged Devices

Introduction
To promote a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information maintained by the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure. IRS Publication 1075 provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Tax Information (FTI). FTI is defined by the IRS as any tax return or return information (and information derived from it) received from the IRS or secondary source.

The US Internal Revenue Service Publication 1075 (IRS 1075) applies to all organizations that process or maintain US Federal Tax Information (FTI). Its purpose is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. The IRS Office of Safeguards is the responsible office that maintains Publication 1075.

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, provides very detailed audit requirements. Publication 1075 documents the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI. The IRS has mapped the IRS Publication 1075 control requirements to the National Institute of Standards and Technology (NIST) control requirements (NIST SP 800-53). FTI is categorized as Sensitive But Unclassified (SBU) information and may contain personally identifiable information (PII).

As a condition of receiving FTI, the receiving organization must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information.

Unmanaged Devices: In Scope for 1075 Compliance but Hard to Secure at Scale
With the proliferation of Internet of Things (IoT) devices and other unmanaged devices in the world, the challenges of an IRS vendor or FTI handling organization to protect its networks and its information, including Federal Tax Information (FTI), will only grow. Any devices that contain this information need to be protected from these IoT threats.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io

Unmanaged IoT devices lack visibility and are hard to secure. They can automatically connect to the internet or other devices, and commonly do not support software agents for centralized management and security. They also can't be patched or don't support a patching process, because patching and security in general was never built into these devices. Instead, manufacturers use open-source operating systems like BusyBox or embedded Linux to speed up the product distribution to market, and as a result, security becomes an afterthought after these devices have already hit the market. In fact, many of these unmanaged devices have default risky behavior like insecure services, hard-coded passwords or automated data transmissions.

Current scanning like NMAP, Network Access Control (NAC) tools or Vulnerability Scanners fail to identify IoT devices and detect IoT–specific vulnerabilities. These network scanners have gaps in device visibility, context and security with unmanaged devices, because they do not tell exactly what the device is, or exactly what other devices are on the same network. This results in the network manager having to conduct a manual IT asset inventory, which is neither efficient nor practical and will be extra overhead that organizations possess neither the time or the headcount to perform on a regular basis. That being said, the requirement to comply with IRS 1075 does not change, and if organizations want to continue to do business with the Internal Revenue Service, they must comply.

An IRS vendor handling federal tax information must safeguard the personal data of taxpayers. Given the valuable and sensitive information a vendor stores, it's critical that vendors stay a step ahead of emerging threats to reduce their cyber risk, and at the same time, maintain compliance with the increasingly stringent regulatory standards including the IRS 1075 based on NIST 800-53.

The critical challenges that an FTI handling vendor face include –

1. Control ID (RA-5) A security solution that monitors and scans for vulnerabilities in the devices and systems on the network that also provides remediation actions, and provides alerting in the event that new vulnerabilities are discovered. In addition, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain sensitive but unclassified information. This in of itself presents a difficult challenge in the need to conduct scanning but also to protect the scanning from breaching privileged access into sensitive information like FTI.

2. Control ID (AC-19) Establish configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices. Control connection of mobile devices.

3. Control ID (SI-4) Monitor the system to detect: Attacks and indicators of potential attacks in accordance with the following monitoring objectives as defined in IT/Cybersecurity monitoring objectives as defined in the agency policy; and Unauthorized local, network, and remote connections. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io

How IoT Secure Helps to meet the security controls laid out in IRS 1075 and more.

1. IoT Secure performs vulnerability assessments by continuously monitoring (and reporting on) every action taken by organizational assets and systems. IoT Secure's vulnerability capability is non-intrusive, doesn't require a network tap, and there are no software agents, so you can rest assured that there will be no breach of privileged access authorization unlike other competing vendors that do require TAPs and installation of software agents.

2. IoT Secure can identify mobile devices, and using either the Block or Smart Block feature, restrict mobile device connections when connected to the network, especially when that network regularly handles FTI.

3. IoT Secure can automatically and without any tuning monitor devices and alert on any malicious or abnormal behavior. IoT Secure automates the work to capture and research each type of unmanaged device's behavior, then building and maintain security rules and tracking any changes to the device communication patterns to monitor the device.

Try it Free in 5 Minutes!

Jump start your compliance within minutes by Securing Your Unmanaged Devices with IoT Secure's Free IRS 1075 Compliance Starter Kit.

Click to Learn More & to Request Your Free IRS 1075 Starter Kit

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io