IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
AC-1 Access Control Policy and Procedures	Procedures to facilitate the implementation of an access control policy and associated access controls. An appropriate Access Control Policy requires verification and the controlling and limiting of connections to and use of external information systems.	IoTSecure enables AC-1 through its SmartBlock feature, allowing you to block devices on your network with a single button press, instantly isolating and securing your device.
AC-4 Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the technical safeguards in place to protect Federal Tax Information (FTI).	IoTSecure provides our customers the capability to monitor FTI-handling devices that are connecting to networks or IP addresses that they should not be connecting to through our cloud portal
AC-5 Separation of Duties	Define system access authorizations to support separation of duties. Separate the duties of individuals to reduce the risk of malevolent activity without collusion. Ensure that only authorized assets and systems processing, storing, accessing, protecting and/or transmitting Federal Tax Information (FTI).	IoTSecure supports separation of duties by empowering its customers to monitor and report on vulnerabilities of devices that may be owned and maintained by a separate business unit and/or handling priviledged information like FTI.
AC-6 Least Priviledge	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. Prevent non-privileged users from executing privileged functions specific to the handling of FTI and capture the execution of such functions in audit logs.	IoTSecure's SmartBlock feature prevents privileged actions from taking place by blocking ports that devices on your network should not even have open, whether it's FTP, Telnet, or SSH. With a single button press, our customers can instantly isolate and secure their devices. This ensures that non-priviledged users not authorized to handle FTI would not have access to devices that are processing FTI data.
AC-18 Wireless Access	Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access. Identify and mitigate risk associated with unidentified wireless access points connected to the network. Monitor for unauthorized wireless access to the information -	IoTSecure provides clear visibility into all network connected devices, including wireless access points, with data and device behavior analytics. IoTSecure also provides visibility into any vulnerabilities, open ports, and unusual activity observed at the device level.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
AC-18 Wireless Access	cont: system and enforce requirements for wireless connections to the information system. Perform both attack monitoring and vulnerability monitoring on the wireless network to support WLAN security	IoTSecure provides clear visibility into all network connected devices, including wireless access points, with data and device behavior analytics. IoTSecure also provides visibility into any vulnerabilities, open ports, and unusual activity observed at the device level.
AC-19 Access Control for Mobile Devices	Establish configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices. Control connection of mobile devices.	IoTSecure 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.
AU-1 Audit and Accountability Policy and Procedures	An organization must develop and document procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability	IoTSecure's product capability directly supports and automates the measures needed to meet this specific control. IoTSecure can be integrated into the development of your policy and procedures for audit and accountability policy.
AU-2 Audit Events	Identify the types of events that the system is capable of logging in support of the audit function. Such events include all accesses or attempts to access an FTI system, including the identity of each user and devices; activities that might modify, bypass, or negate IT security safeguards; Security-relevant actions associated with processing FTI; Any interaction with FTI through an application; Privileged user actions; Access to the system; and System and data interactions.	IoT allows our customers to query data with regard to devices, threats, and vulnerabilities, allowing analysis and reporting on suspicious or unusual activity. This information can also be exported to SIEMs or other reporting tools through our REST API.
AU-3 Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.	Our Cloud Portal will provide the specific information on the event type, whether it's an exploitable IoT detection, activity of network hopping, as well as the specific date time group of the event.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
AU-4 Audit Storage Capacity	Allocate audit log storage capacity to accommodate the retention of audit records for the retention period	IoTSecure will provides log storage of the event history of your IoT assets. IoTSecure has integrations with all major SIEMs, including Splunk. IoT Secure also has a REST API that can feed data into a customized SIEM residing in the customer environment.
AU-6 Audit Review, Analysis and Reporting	a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; b. Report findings to the individual(s) specified within the agency's incident response procedures; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	IoTSecure automatically analyzes device, network, and security information and alerts when it detects critical indicators of compromise. Information can also be sent to a SIEM for external analysis and alerting or through a REST API to your data repository.
AU-7 Audit Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: likelihood of potential inappropriate access or unauthorized disclosure of FTI. Events of interest is the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.	IoTSecure maintains a record of network transmissions for every device to every internal and external destination, on every port, on every protocol. This record can be critical to investigations of unlawful or unauthorized system activity. Our cloud portal allows for the exporting of information to spreadsheets or summarization. We also provide weekly reports that provide the most up to date information on new vulnerabilities detected on assets connected to your network.
AU-8 Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet agency-defined granularity and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	IoTSecure's event monitoring system stores the time stamps in UTC but automatically uses DTG Time Stamps of Year:Month:Date:Hour:Minute: Second at your local time time zone, and includes an entire timeline of when device was profiled, associated IP addresses with devices, as well as time stamp history of vulnerabilities found.

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
AU-9 Protection of Audit	Protect audit information and audit logging tools from unauthorized access, modification, and deletion. Authorize access to management of audit logging functionality to only authorized system administrators	IoTSecure can support implementation as part of a complete system.
AU-11 Audit Record Retention	Retain audit records seven (7) years to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	IoTSecure will retain records for any period that you designate. Please contact sales on the year retention requirement that you have and we can support.
AU-12 Audit Generation	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems that receive, process, store, access, protect and/or transmit FTI; Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	IoTSecure provides unique value because it automatically inspects devices for vulnerabilities both as they connect to the network and continuously and it does so safely without crashing devices. This allows vulnerability testing on unmanaged devices and fills a gap with traditional vulnerability scanners which commonly crash these devices and leave them untested on the network.
CA-1 Assessment, Authorization and Monitoring Policy and Procedures	Procedures to facilitate the implementation of the security and privacy assessment, authorization and monitoring policy and the associated security and privacy assessment, authorization, and monitoring controls	IoTSecure's product capability directly supports and automates the measures needed to meet this specific control. IoTSecure can be integrated into the development of your policy and procedures for assessment as well as for monitoring policy and procedures.
CA-2 Assessments	Develop a control assessment plan that describes the scope of the assessment including: (1) Controls and control enhancements under assessment; (2) Assessment procedures to be used to determine control effectiveness; & (3) Assessment environment, assessment team, and assessment roles and responsibilities; Produce a control assessment report that document the results of the assessment	IoTSecure provides a threat check report that you can incorporate as part of you control assessment plan.

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
CA-5 Plan of Action and Milestones	Develop a plan of action and milestones for the system to document the planned remediation actions of the agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; Update existing plan of action and milestones on a quarterly basis, at a minimum, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities. Supplemental Guidance: The POA&M must comprise of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, access, protect and/or transmit FTI. **Control Enhancements:** (IRS-Defined): Agencies must ensure that the individual and/or office responsible for correcting each weakness is identified in the appropriate POA&M. (IRS-Defined): Agencies must enter all new weaknesses into appropriate POA&Ms within two (2) months for weaknesses identified during assessments.	IoTSecure integrates with ITSM solutions like Service Now to trigger the appropriate workflow for a given deficiency or vulnerability. Our alerts also provide recommended actions with regard to handling of the device or asset.
CA-7 Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy	IoTSecure delivers passive and continuous monitoring of your network assets, which can provide a clear picture of the effectiveness of controls (e.g., speed of patching systems, connections to malicious URLs, accuracy of VLAN assignments, etc.), across the organization.
CA-9 Internal System Connections*	Authorize internal connections of information system components or classes of components to the system; Terminate internal system connections after agency-defined conditions	IoTSecure employs the Block Feature to block all access to individual device(s) on your network, while our Smart Block can allow enterprise customers like you the ability to block open ports, thus reducing the threat surface to devices on your network, and by extension your network.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
CM-1 Configuration Management Policy and Procedures	Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls	IoTSecure automatically discovers, tracks and provides detailed inventories of all devices. IoTSecure identifies devices by category, type, make, model, OS, ports and network so you always have a complete context and detailed inventory of devices, without any manual work.
CM-2 Baseline Configuration	Develop, document, and maintain under configuration control, a current baseline configuration of the system	IoTSecure automatically detects insecure configurations on unmanaged devices such as default credentials and unwanted/unnecessary services without any disruption to devices or to the network, which is common with that traditional security tools and scanners. Additionally, IoTSecure identifies risky device communications that can be compared against the inventory baseline once setup is complete.
CM-8 System Component Inventory	Develop and document an inventory of system components that: Accurately reflects the system; Includes all components within the system; Is at the level of granularity deemed necessary for tracking and reporting; and Includes the following information to achieve system component accountability. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	IoTSecure can document the full asset inventory of your network(s). This information includes manufacture, device type, IP address, device name, device operating system, as well as device manufacturer country of origin.
CM-9 Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the systems development lifecycle (SDLC) and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management;	IoTSecure automatically discovers, tracks and provides detailed inventories of all devices. IoTSecure identifies devices by category, type, make, model, OS, ports and network so you always have a complete context and detailed inventory of devices, without any manual work. This can all be incorporated as part of your Configuration Management Plan.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
IA-5 Authenticator Management	Manage system authenticators through specific measures, to include Changing default authenticators prior to first use.	IoTSecure can identify default passwords on network-connected devices.
IR-1 Incident Response Policy and Procedures	Procedures to facilitate the implementation of the incident response policy and the associated Incident response controls	The IoTSecure Cloud Portal has an alerting capability built in that provides alerts on devices in your network, letting you know of any suspicious activity as well as recommended actions to undertake as a result of the particular alert, whether it be a vulnerability that was discovered or suspected activity that requires incident response such as suspected DNS tunneling.
IR-4 Incident Handling	Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery	IoTSecure's alerting system and index can utilized as part of incident handling procedures, making your incident handling procedure more robust especially as it pertains to IoT Devices.
IR-7 Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	The IoTSecure Cloud Portal has an alerting capability built in that provides alerts on devices in your network, letting you know of any suspicious activity as well as recommended actions to undertake as a result of the particular alert, whether it be a vulnerability that was discovered or suspected activity that requires incident response such as suspected DNS tunneling.
IR-8 Incident Response Plan	Develop an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability and describes the structure and organization of the incident response capability.	IoTSecure's alerting system and index can incorporated as part of your Incident Respond Plan, and be integrated into your incident response capability.
MP-1 Media Protection Policy and Procedures	Procedures to facilitate the implementation of the media protection policy and the associated media protection controls	IoTSecure can support implementation as part of a complete system. IoT Secure and help you segregate your devices handling FTI, allowing you to focus on those specific devices.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
MP-2 Media Access	Restrict access to digital and/or non-digital media containing FTI to authorized individuals.	IoTSecure can support implementation as part of a complete system. IoT Secure and help you segregate your devices handling FTI, allowing you to focus on those specific devices, and supporting you in policies in restricting access to FTI on system media to authorized users.
PE-1 Physical and Environmental Policy and Procedures	Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; Designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals and communications equipment	IoTSecure can support implementation as part of a complete system.
PM-4 Plan of Action and Milestones Process*	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation	IoTSecure provides you a full picture of your asset inventory and the vulnerability oversight into your assets. Recommended actions are provided on any vulnerabilities and can directly help support your plan of action and milestones process.
PM-5 System Inventory *	Develop and update continually an inventory of organizational systems	IoTSecure provides a full asset inventory of your IoT assets and automates discovery of the addition of new assets connecting into your network.
PM-9 Risk Management Strategy*	Develop a comprehensive strategy to manage: Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems	IoTSecure's product suite and alerting system can incorporated as part of your Risk Management Strategy.
PM-12 Insider Threat Program*	Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integrat -ion and analysis of both technical and non-technical information to identify potential insider threat concerns.	IoTSecure ensures you have full visibility into all assets connecting into your network. If there's any unauthorized or suspicious activity being carried out by these devices, IoTSecure can serve as an alert warning outpost for insider threat activity utilizing IoT devices.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
RA-1 Risk Assessment Policy and Procedures	Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls	IoTSecure's alerting system and index can incorporated as part of your Risk Assessment Policy, and our product suite can be integrated into your Risk Procedures.
RA-3 Risk Assessment	Conduct a risk assessment, including: Identifying threats to and vulnerabilities in the system; Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; c. Assess supply chain risks associated with Federal Tax Information.	IoTSecure provides unique value because it automatically inspects devices for vulnerabilities both as they connect to the network and continuously and it does so safely without crashing devices. This allows vulnerability testing on unmanaged devices and fills a gap with traditional vulnerability scanners which commonly crash these devices and leave them untested on the network.
RA-5 Vulnerability Scanning	Monitor and scan for vulnerabilities in the system and hosted applications every thirty (30) days, prior to placing a new information system on the agency network, to confirm remediation actions, and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: Enumerating platforms, software flaws and improper configurations; Formatting checklists and test procedures; and Measuring vulnerability impact. Supplemental Guidance: Automated security scanning of assets (including wireless networks) for inventory, configuration, and vulnerability data, including at the application-level, must be included in monthly required vulnerability scans Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain classified or controlled unclassified information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.	IoTSecure performs vulnerability assessments by continuously monitoring (and reporting on) every action taken by organizational assets and systems. IoTSecure'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.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
RA-7 Risk Response*	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	IoTSecure provides recommended actions as a result of vulnerability discoveries, thus supporting this control in responding to any security-related findings.
SA-5 Information System Documentation	Obtain or develop administrator documentation for the system, system component, or system service that describes: Effective use and maintenance of security and privacy functions and mechanisms; and Known vulnerabilities regarding configuration and use of administrative or privileged functions.	IoTSecure can provide you the full inventory and documentation of vulnerabilities detected on your IoT assets.
SI-2 Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner. Organizations identify systems affected by software flaws including potential vulnerabilities resulting from those flaws and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities and system error handling. By incorporating flaw remediation into ongoing configuration management processes, required remediation actions can be tracked and verified.	IoTSecure ensures passive and continuous monitoring of all network-connected devices for timely reporting and remediation.
SI-4 System Monitoring	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.	IoTSecure 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.

IoTSecure™

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

IRS 1075 Controls Addressed By IoTSecure

Control ID	Control Description	How IoTSecure Maps
SR-1 Supply Chain Risk Management Policy and Procedures	Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls	IoTSecure's manufacturer index and asset manufacturer country of origin provides you visibility into where your assets are sourced from so that you can incorporate our product suite and capability into your supply chain risk management policy and procedures.
SR-2 Supply Chain Risk Management Plan	Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: Information systems that process, store, or transmit FTI	IoTSecure's manufacturer index and asset manufacturer country of origin provides you visibility into where your assets are sourced from so that you can incorporate our product suite and capability into your supply chain risk management plan.

IoTSecure™

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