



White Paper

From Mandate to Action: Responding to CISA's OT Asset Inventory Guidance with ConsoleWorks

Phone: +1.800.695.1258

Mail: info@ConsoleWorks.com

Website: www.ConsoleWorks.com

From Mandate to Action: Responding to CISA's OT Asset Inventory Guidance with ConsoleWorks

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with key partners like the NSA and DOE, recently released a joint guidance document: *Foundations for OT Cybersecurity: Asset Inventory*.

You can find the document here:

https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf

CISA's guidance signals a turning point. Asset inventory is no longer a passive spreadsheet exercise — it's the foundation of modern OT cybersecurity. It's not just an operational necessity, it is a **cybersecurity imperative**.

At TDi Technologies, we couldn't agree more. The guidance validates years of investment and innovation behind **ConsoleWorks Asset Inventory** — our unified approach to OT visibility, intelligence, and risk-informed action.

Translating CISA Requirements into Real-World Capability

CISA outlines essential requirements such as maintaining an accurate, centralized, and secure inventory of all OT assets — including not just devices, but software, users, ports, and firewall rules. It emphasizes:

- Lifecycle management and change tracking
- Categorization by criticality and function
- Network zone mapping
- Periodic review and ownership assignment

ConsoleWorks Asset Inventory was built with these principles in mind. Our platform automatically ingests and normalizes asset metadata from multiple sources, applies customizable classification schemes, and organizes assets into an extensible inventory model aligned to real-world infrastructure and cyber risk posture. Every asset — whether physical or virtual — becomes traceable, contextualized, and actionable.

But, ConsoleWorks goes beyond just Asset Inventory, it then uses the asset inventory data to evaluate your environment, at any level, for security, compliance, and operational risk. Since its integrated with ConsoleWorks SRA, action can be immediately taken. This is where the real value is realized. And ConsoleWorks continuously enables this close-loop process.

ConsoleWorks Mapping to CISA Guidance

CISA Guidance Requirement		Rationale / Source from the CISA Guidance	ConsoleWorks Asset Inventory Capability
1	Create and maintain an OT asset inventory	An OT asset inventory—an organized, regularly updated list of an organization’s OT systems, hardware, and software—is foundational to designing a modern defensible architecture.	ConsoleWorks builds a real-time inventory by ingesting, correlating, and normalizing data from passive discovery tools and its own active collections.
2	Include essential asset attributes (e.g., hostname, IP, MAC, model, OS)	A full list is outlined on p.8: hostname, IP, MAC, manufacturer, model, OS, location, ports/services, user accounts, etc.	ConsoleWorks captures and stores critical fields in structured inventory components including Asset, Network, Software, Hardware, Patches, Antivirus, and User views.
3	Develop and apply a taxonomy to classify assets	An OT taxonomy is a categorization system used to organize and prioritize OT assets...	ConsoleWorks uses rule-based mappings and override logic to organize assets by type, classification, and function, providing a normalized structure for each tool source. Additional groupings for others such as Process can be easily defined.
4	Classify assets by criticality or function	Supports risk-based management: Assets are classified based on their importance...	Inventory Asset records include criticality, classification, function, process, and other metadata to inform risk scoring and compliance.
5	Use zones and conduits (ISA/IEC 62443) to group assets and communication paths	Organizes assets into Zones and Conduits... to ensure authorized data can pass and to align security requirements.	Inventory Network stores zone designations for each interface and correlates these to asset records for segmentation-aware visibility.
6	Identify data sources to enhance inventory (e.g., vendor manuals, configs)	Identify sources of data for each asset... that may enhance the inventory.	ConsoleWorks accepts data from multiple tools (Tenable, Palo Alto, etc.) and captures the source of each mapping through tool designations and plugin links.
7	Store inventory in a centralized database with appropriate security controls	Establish a centralized database... implementing security controls to ensure data protection.	ConsoleWorks Asset Inventory resides within the ConsoleWorks platform with role-based access control, encryption, and auditability.
8	Implement life cycle management with change control and update triggers	Develop policies for managing assets throughout their life cycle... requiring inventory updates for introduction or removal of devices.	ConsoleWorks uses Last Seen, Discovered Date, and “IsRemoved” fields for lifecycle status tracking, and supports override logic for lifecycle corrections. Others can easily be added.
9	Designate ownership of inventory accuracy and updates	Identify asset inventory owners to oversee updates and validate asset classifications.	Asset records include ownership fields such as Managed By and Location; Inventory governance is supported by role-based access and data review workflows.
10	Periodically review and update inventory and taxonomy	Periodically review and update the taxonomy... gather feedback from stakeholders.	ConsoleWorks supports data validation via rules, overrides, and export/review workflows. Taxonomy can be updated via rule configuration.
11	Train staff in asset management practices, tools, and procedures	Train staff in asset management practices...	ConsoleWorks provides structured views of inventory and exportable data for use in training and review.
12	Analyze OT spare parts inventory for operational reliability	Determine whether the stockpile of spare OT components sufficiently covers the critical assets identified.	While not a spare parts tracker, ConsoleWorks supports identification of hardware models and usage across assets to inform redundancy planning.

ConsoleWorks Augmentation vs CISA

While the CISA guidance outlines a strong foundation for OT asset inventory, there are critical operational and security gaps it does not explicitly address. ConsoleWorks goes beyond this guidance by embedding actionable intelligence, real-time correlation, and remediation capabilities directly into the asset inventory workflow. The following table highlights additional requirements—derived from ConsoleWorks’ design principles and real-world customer needs—that complement and extend the value of CISA’s recommendations. These capabilities represent the difference between a static inventory and an intelligent, operationally integrated one.

Requirement		Rationale	ConsoleWorks Asset Inventory Capability
13	Correlate software, users, hardware, network interfaces, and firewall rules to each asset	Enables a full system-of-systems view, allowing insight into configuration and contextual risk	ConsoleWorks structures inventory into normalized components (Inventory Asset, Inventory Software, Inventory Users, etc.), all linked to a central asset record.
14	Track user accounts and login behavior per asset	User access visibility is critical for identity-based risk scoring and auditing	ConsoleWorks Inventory Users tracks account ID, auth type, MFA status, unsuccessful logins, and domain per asset.
15	Identify externally accessible interfaces and network segments	Required for evaluating exposure, especially for remote access or internet-facing assets	Inventory Network includes NAT IPs, externally accessible flags, zone membership, and MAC/IP mapping.
16	Track presence and state of endpoint security tools (e.g., antivirus) per asset	Supports detection of control coverage gaps	Inventory Antivirus component stores AV name, version, scanning status, and signature update date.
17	Normalize tool data across multiple sources into a unified model	OT environments often use multiple tools with inconsistent data	ConsoleWorks uses rule-based mapping to normalize and correlate multi-source data into a unified asset structure.
18	Detect and track policy violations and configuration drift	Continuous compliance requires more than static inventory	ConsoleWorks detects missing or changed attributes based on expected values, rules, and override logic.
19	Support override logic for manual validation or correction of tool data	Some data requires human reconciliation	Override support exists for all inventory components to ensure human-reviewed truth is preserved alongside tool data.
20	Attribute assets to organizational ownership or management roles	Needed for accountability and routing of actions	Ownership fields (e.g., Managed By) in Inventory Asset support designation of responsibility.
21	Support risk scoring at the asset level based on security control coverage	Enables prioritization of remediation and policy enforcement	Risk scores are calculated from answers to security / regulatory-based questions mapped to each asset’s control coverage.
22	Retain historical data for audit and trend analysis	OT asset risk is not static—change tracking is essential	ConsoleWorks stores Last Seen, Install Dates, Removal Flags, and update history for each inventory component.
23	Enable immediate remediation of compliance or security issues from within the inventory platform	A truly actionable asset inventory should not only identify out-of-compliance conditions but also support rapid and auditable remediation. The ability to move directly from detection to resolution reduces mean time to respond (MTTR), limits risk exposure, and improves audit readiness.	ConsoleWorks integrates its Secure Remote Access (SRA) directly with the Asset Inventory. When an asset is flagged (e.g., missing a patch, misconfigured setting, failed control), authorized users can initiate a secure session directly from the inventory record to perform remediation — such as updating software, restoring configuration, or applying patches. All actions are recorded for compliance traceability.

It's Not Just Inventory — It's Intelligence with Context

The CISA guide stops at visibility. Unlike traditional CMDBs or passive discovery tools, ConsoleWorks goes further. It connects each inventory element with the following:

- Secure access pathways
- Known vulnerabilities
- User and identity information
- Configuration drift
- Policy violations
- Real-time event activity

This rich context turns a static inventory into a dynamic **Cybersecurity / Compliance / Operational Risk Profile**, enabling teams to **prioritize and act** with confidence. It provides the insight that drives action.

When ConsoleWorks detects a misconfiguration, missing patch, or policy deviation, it doesn't just alert. Thanks to our **embedded Secure Remote Access (SRA)**, if appropriate, authorized users can immediately initiate a secure session to remediate the issue — directly from the inventory record — while maintaining full auditability and policy compliance.

Cybersecurity / Regulatory Mapping Built In

ConsoleWorks doesn't operate in a vacuum. Our risk model maps directly to the **Secure Controls Framework (SCF)** (<https://securecontrolsframework.com>)— the industry-standard overlay that ties security controls to multiple regulations including NIST CSF, NERC CIP, CMMC, and many more. By anchoring asset intelligence to SCF, we not only meet the **letter of compliance** but support the **spirit of resilience**.

With ConsoleWorks, organizations get a future-ready asset inventory that is:

- Comprehensive
- Contextual
- Continuous
- Connected to action

If you're ready to turn data into decisions — we're ready to help.

[Request a Demo] or **[Download the Whitepaper]** to see how ConsoleWorks can transform your OT visibility into intelligence.