FORESCOUT

This document is intended to provide information on how pipeline owners/operators can address the United States Transportation Security Administration's (TSA) security directive aimed at hardening this critical infrastructure sector.

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
Identify	**Asset Management**		
	Establish and document policies and procedures for assessing and maintaining configuration information, for tracking changes made to the pipeline cyber assets, and for patching/upgrading operating systems and applications. Ensure that the changes do not adversely impact existing cybersecurity controls.	Employ mechanisms to maintain accurate inventory and to detect unauthorized components.	The Forescout platform continuously provides an up-to-date asset inventory with detailed device information (vendor/model information, firmware version, serial numbers etc.), vulnerabilities and configuration change logs for all network assets. This information is obtained through purpose-built, continuous passive monitoring and optional active scanning techniques for OT/ICS assets. Furthermore, users can leverage our asset baselining capabilities to define device compliance policies (i.e., desired configuration and open ports), identify and report on compliance deviations in real time.
	Develop and maintain a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows.	Review network connections periodically, including remote and third-party connections. Develop a detailed inventory for every endpoint.	The Forescout platform passively monitors all network communications to provide real-time visibility into assets and flows. Users can leverage interactive device mapping to understand communication traffic flow between devices, volume and protocol employed. Advanced visual analytics provide a complete representation of flows for both real-time and forensic analysis. Traffic flows can be mapped to logical taxonomy of users, applications, services and devices to understand

Baseline Security Measures	Enhanced Security Measures	Forescout Solution
		current communication patterns, and define and enforce segmentation policies.
Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months.		The Forescout platform provides agentless, real-time asset discovery, profiling, classification/prioritization and HW/ SW inventory views across both IT and OT/ICS environments. Deep Packet Inspection engines automatically determine the role for each device on the network(s), along with providing asset inventory information - such as model number, firmware version and serial number (if available) within the network protocols. All asset inventory data is available for export and via API to be consumed by asset repositories, compliance reporting systems or other systems.
Business Environment		
Ensure that any change that adds control operations to a non-critical pipeline cyber asset results in the system being recognized as a critical pipeline cyber asset and enhanced security measures being applied.		The Forescout platform tracks and validates any changes to asset software or firmware and maintains an accurate device change log. It further ensures device compliance and validates changes performed to any Windows OS based system in real-time and with the correct user privileges.
Governance		
Establish and distribute cybersecurity policies, plans, processes and supporting procedures commensurate with the current regulatory, risk, legal		N/A

FORESCOUT

Baseline Security Measures	Enhanced Security Measures	Forescout Solution
and operational environment.		
Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 36 months, or when there is a significant organizational or technological change. Update as necessary.	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 12 months, or when there is a significant organizational change. Update as necessary.	N/A
Risk Management Strategy		
Develop an operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks.		The Forescout platform provides detailed OT/ICS asset information, security and operational risk scores for each device. It continuously monitors and alerts on undesired communication between enterprise and control system networks. These capabilities combined with Forescout's integration with configuration management/CMDB solutions, SIEMs, data analytics and compliance reporting tools enable preventative and predictive device maintenance with superior operational and risk-related information.
Risk Assessment		
Establish a process to identify and evaluate vulnerabilities and compensating security controls.	Ensure threat and vulnerability information received from information sharing forums and sources are made available to those responsible for assessing and determining the appropriate course of action.	The Forescout platform's extensive OT/ICS vulnerability database and analysis views allow organizations to quickly identify critical vulnerabilities that impact devices and networks. It continuously monitors, logs and detects potential OT/ICS threats or deviations from baseline

FORESCOUT

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
			communications by combining signature, behavioral and anomaly-based detection techniques. The platform monitors for known threats internally and externally, and when a threat is detected, it can provide automated controls to manage network access.
Protect	**Access Control**		
	Establish and enforce unique accounts for each individual user and administrator, establish security requirements for certain types of privileged accounts, and prohibit the sharing of these accounts. In instances where systems do not support unique user accounts, then implement appropriate compensating security controls (e.g., physical controls).	Restrict user physical access to control systems and control networks through the use of appropriate controls. Employ more stringent identity and access management practices (e.g., authenticators, password- construct, access control).	The Forescout platform can see when an OT/ICS asset is accessed remotely and, depending on the type of access, who is logging into the device. Furthermore, the platform allows for granular Role Based Access Control policies to limit access and privileges to information collected by the platform, for both local and externally authenticated users (e.g., LDAP/AD). Forescout's integration with Privileged Access Management tools can help prevent privileged credential misuse and unauthorized network access
	Ensure that user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company.		
	Establish and enforce access control policies for local and remote users. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections.	Monitor physical and remote user access to critical pipeline cyber assets.	
	Ensure appropriate segregation of duties is in place. In instances where this		The Forescout platform can detect changes made to an OT/ICS asset by a user, such as

FORESCOUT

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
	is not feasible, apply appropriate compensating security controls.		new firmware, program or configuration downloads, as well as changes made to IT endpoints managed by the Forescout platform. The platform's segmentation capabilities provide the ability to monitor and segment access across devices, networks or sites.
	Change all default passwords for new software, hardware, etc., upon installation. In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), implement appropriate compensating security controls (e.g., administrative controls).	Employ mechanisms to support the management of accounts.	The Forescout platform detects the use of default credentials or if they haven't been changed. In addition, the platform can identify if an active directory user's password has expired and can respond in a variety of ways. The platform enables compensating controls including passive, real-time network monitoring and dynamic network segmentation.
Protect	**Awareness and Training**		
	Ensure that all persons requiring access to the organization's pipeline cyber assets receive cybersecurity awareness training.	Provide role-based security training on recognizing and reporting potential indicators of system compromise prior to obtaining access to the critical pipeline cyber assets.	N/A
	Establish and execute a cyber-threat awareness program for employees. This program should include practical exercises/testing.		
	Data Security and Information Protection		
	Establish and implement policies and procedures to ensure data protection measures are in place, including identifying critical data and establishing classification of different types of data, establishing specific handling		The Forescout platform stores and preserves information fully on-premises, ensuring secure data protection (at rest & in transit) for IT, OT and IoT networks. At rest, data is stored in a secure environment with

FORESCOUT

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
	procedures, and protections and disposal.		underlying code that is continuously tested against attacks and vulnerabilities. In transit data is secured via multiple methods.
	Protective Technology		
	Segregate and protect the pipeline cyber assets from enterprise networks and the internet using physical separation, firewalls and other protections.		The Forescout platform monitors all OT, IT and IOT devices to ensure real-time alerting should a device fall out of it established segment or established data flows. The platform also automatically manages the network controls according to established policies.
	Regularly validate that technical controls comply with the organization's cybersecurity policies, plans and procedures, and report results to senior management.		The Forescout platform's industrial threat library and anomaly detection engines monitor communications to detect weak security posture (e.g., default credentials or insecure protocols) and intrusion attempts along with recommendations on response actions. The platform enables the establishment of control policies to restrict access to the network and its devices, and continuously monitor devices for policy compliance and violation to segmentation policies.
	Implement technical or procedural controls to restrict the use of pipeline cyber assets for only approved activities.		
	Anomalies and Events		
Detect	Implement processes to generate alerts and log cybersecurity events in response to anomalous activity. Review the logs and respond to alerts in a timely manner.		The Forescout platform provides real-time visibility into network communications, supporting the creation of informed network access controls for OT/ICS devices. In addition, it detects weak security posture (e.g., default credentials or insecure protocols) and intrusion attempts

Baseline Security Measures	Enhanced Security Measures	Forescout Solution
		at their earliest stages, providing recommendations on response actions. It also logs successful and failed authentication attempts for complete historical records of host activities including firmware changes, new protocols, new roles, etc.
Security Continuous Monitoring		
Monitor for unauthorized access or the introduction of malicious code or communications.		The Forescout platform enables field device access monitoring, alerting, and reporting on authorized or unauthorized engineering, contractor, or integrator activities, helping to ensure operational and business policies are adhered to. All this information is stored, in detail and with associated risk ratings, in the asset inventory.
Conduct cyber vulnerability assessments as described in your risk assessment process.	Utilize independent assessors to conduct pipeline cyber security assessments.	The Forescout platform provides real-time visibility into all network communications allowing organizations to harden their network access controls, ensuring least privilege. The platform also logs all successful and failed authentication attempts, file operations, and maintains a complete history of all host activities, including firmware changes. The Forescout platform features an extensive database of known OT/ICS vulnerabilities and related views to quickly identify areas that may negatively affect critical network devices. Forescout's Industrial Threat Library (ITL) features more than 2100+ behavioral-based threat indicators, which combined with the platform's

FORESCOUT

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
Detect			advanced anomaly detection capabilities allow for identification of both known and unknown (zero-day) threats.
	Detection Processes		
	Establish technical or procedural controls for cyber intrusion monitoring and detection.		The Forescout platform detects weak security posture (e.g., default credentials or insecure protocols) and intrusion attempts at their earliest stages, providing recommendations on response actions. All alerts, user and network event logs can be sent to SIEMs, log management, and correlation engines.
	Perform regular testing of intrusion and malware detection processes and procedures.		N/A
	Response Planning		
Respond	Establish policies and procedures for cybersecurity incident handling, analysis and reporting, including assignment of the specific roles/tasks to individuals and teams.	Conduct cybersecurity incident response exercises periodically.	The Forescout platform includes case management capabilities to group alerts which are part of a new or ongoing investigation effort, to support the incident investigation and handling process.
	Establish and maintain a cyber-incident response capability.	Establish and maintain a process that supports 24 hours a day cyber incident response.	N/A
	Communications		
	Report significant cyber incidents to senior management; appropriate federal, state, local, tribal, and territorial (SLTT) entities; and applicable ISAC(s).	Pipeline operators should follow the notification criteria in Appendix B	N/A

FORESCOUT

	Baseline Security Measures	Enhanced Security Measures	Forescout Solution
Recover	**Mitigation**		
	Ensure the organization's response plans and procedures include mitigation measures to help prevent further impacts.		N/A
	Recovery Planning		
	Establish a plan for the recovery and reconstitution of pipeline cyber assets within a timeframe to align with the organization's safety and business continuity objectives.		The Forescout platform can ensure replaced or recovered assets meet established policies and criteria that have been established.
	Improvements		
	Review the organization's cyber recovery plan annually. Update as necessary.		N/A

Source: TSA Pipeline Security Guidelines Facility Security Measures - March 2018 (with Change 1 (April 2021))