Perspecta Labs SecureSmart™ Critical Infrastructure Monitoring Solution — Cyber Catalyst Designation

Perspecta Labs' Secure**Smart**™ critical infrastructure monitoring solution has been designated a 2019 Cyber Catalyst solution. It addresses cyber risks borne by operators of field control systems and critical infrastructure, typically electric, gas, drinking water, water treatment, oil and gas, industrials, and traffic control systems for surface transportation.

A monitoring system for today's smart control networks and Supervisory Control and Data Acquisition systems (SCADA), Secure**Smart** is a comprehensive critical infrastructure and Industrial Control System (ICS) defense that provides operators with real-time visibility into the health of their networks, early warning of intrusion, and tools to diagnose and troubleshoot problems in field control networks.

Secure**Smart** deploys patented sensors in wireless field networks and traditional control networks to passively intercept control traffic and process telemetry. Intelligent applications perform deep-packet analysis, time series traffic analysis, protocol and session state analysis, endpoint behavioral analysis, and telemetry consistency analysis of multiple traffic streams from physical through application layers. It offers active, protocol-specific defense by either dropping anomalous communications packets or ending suspicious sessions.

Secure**Smart** mitigates risks of:

- Security and configuration flaws in the wireless, software, network and hardware aspects of field operations technology.
- Unauthorized control of cyber-physical assets that could result in safety and physical consequence.
- Compromise of Personally Identifiable Information and privacy data.
- Operator revenue loss and theft of service.
- Cybersecurity-triggered service outages that might result in regulatory fines and reputation harm.
- Ransomware attacks.
- Unauthorized use of operator assets and networks for illegal activities, crime, and terrorism.

Developed and tested with the assistance of the Department of Energy and Defense Advanced Research Projects Agency, Secure**Smart** is used by major utilities to monitor advanced metering and distribution automation infrastructure across the US. It is deployable as a self-managed product solution or a managed service with rapid deployment and minimal customer overhead.

Perspecta Labs positions Secure**Smart** as ideal for enterprises and municipalities with ICS networks, Internet of Things (IoT) and smart city deployments, smart energy grids, smart building controls, industrial production line control protocols and vehicular traffic control systems.

**Product information provided by Perspecta Labs*

Why Perspecta Labs' SecureSmart™ Critical Infrastructure Monitoring Solution is a Cyber Catalyst-Designated Solution

Cyber Catalyst participating insurers rated the Secure**Smart**™ Critical Infrastructure Monitoring Solution highest on the criteria of cyber risk reduction and efficiency.

In their evaluation, the insurers characterized it as:

- "Strong capability within the utilities industry to monitor distributed network devices. ICS/SCADA component is a great, efficient fit for manufacturing and industrial users."
- "Unique approach to standardization seems to bring a consistent monitoring approach to an industry heavily reliant on legacy systems and controls. Powerful reporting and dashboarding capabilities."
- "Different tiers of deployment make implementation easy while yielding large amounts of sensor data to conduct alerts and analysis."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst-designated products or services in accordance with certain "implementation principles" that have been developed by the insurers with vendors of Cyber Catalyst-designated solutions.

The implementation principle for the Secure**Smart**™ Critical Infrastructure Monitoring Solution is:

- Secure**Smart**™ Monitoring Solution has been installed and configured to monitor and analyze associated traffic for security and operational anomalies across critical control infrastructure and wireless low-power wide area field networks. Monitored infrastructure and Secure**Smart** are updated with patches within 30 days of release.

Evaluation Process

Applications for evaluation of cybersecurity solutions were accepted from March 26 through May 5, 2019. More than 150 cybersecurity offerings, spanning a broad range of categories from hardware to messaging security to IoT security, were submitted for evaluation. Cyber Catalyst participating insurers evaluated eligible solutions along six criteria:

1. *Reduction of cyber risk.*
2. *Key performance metrics.*
3. *Viability.*
4. *Efficiency.*
5. *Flexibility.*
6. *Differentiating features.*

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight participating insurers, which voted independently. Neither Microsoft — which served as technical advisor — nor Marsh participated in Cyber Catalyst℠ designation decisions.

The next Cyber Catalyst program is expected to open in 2020.

For more information on the Cyber Catalyst 2019 designated solutions or the program, visit the Cyber Catalyst pages at www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit marsh.com, or contact your Marsh representative.

For more information about Perspecta Labs's Secure**Smart**™ Critical Infrastructure Monitoring Solution, visit https://www.perspectalabs.com/critical-infrastructure.

2019 CYBER CATALYST DESIGNATED SOLUTIONS

In the inaugural Cyber Catalyst program, 17 cybersecurity products and services have been designated as Cyber Catalyst solutions. More information about all the 2019 Cyber Catalyst-designated cybersecurity solutions is at www.marsh.com/cybercatalyst.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.